

ZyXEL AG-225H v2

802.11a/g Wi-Fi Finder & Wireless USB Adapter

User's Guide

Version 1.00

Edition 1

6/2006

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is lowercase and the "XEL" is uppercase. The letters are closely spaced and have a slight shadow effect.

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

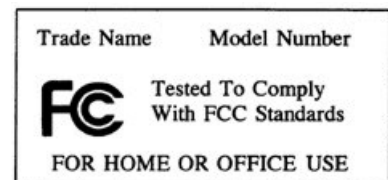
This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Caution

- 1 The 802.11g Wireless LAN Adapter has been tested to the FCC exposure requirements (Specific Absorption Rate).
- 2 The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
- 3 This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.



注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

METHOD	SUPPORT E-MAIL	TELEPHONE^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
		+48 (22) 333 8251		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

a. "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright	3
Certifications	3
ZyXEL Limited Warranty	5
Customer Support.....	6
Table of Contents	9
List of Figures	13
List of Tables	15
Preface	17
Chapter 1	
Getting Started	19
1.1 About Your AG-225H v2	19
1.2 Application Overview	19
1.2.1 Station Mode	19
1.2.1.1 Infrastructure	19
1.2.1.2 Ad-Hoc	20
1.2.2 Access Point Mode	21
1.2.3 Changing AG-225H v2 Mode	21
1.3 AG-225H v2 Hardware and Utility Installation	22
1.3.1 ZyXEL Utility Icon	22
1.4 Configuration Methods	22
1.4.1 Enabling WZC	22
1.4.2 Accessing the ZyXEL Utility	23
Chapter 2	
Tutorial	25
2.1 Connecting to a Wireless LAN	25
2.2 Creating and Using a Profile	27
2.3 Configuring the AG-225H v2 as an AP	31
Chapter 3	
Wireless LAN Network.....	33
3.1 Wireless LAN Overview	33
3.2 Wireless LAN Security	34

3.2.1 Hide SSID	34
3.2.2 MAC Address Filter	34
3.2.3 User Authentication and Encryption	35
3.2.3.1 WEP	35
3.2.3.2 IEEE 802.1x	36
3.2.3.3 WPA and WPA2	36
Chapter 4	
Wireless Station Mode Configuration	39
4.1 Wireless Station Mode Overview	39
4.1.1 ZyXEL Utility Screen Summary	39
4.2 The Link Info Screen	40
4.2.1 Trend Chart	41
4.3 The Site Survey Screen	42
4.3.1 Security Settings	43
4.3.1.1 WEP Encryption	43
4.3.1.2 WPA-PSK/WPA2-PSK	44
4.3.1.3 WPA/WPA2	45
4.3.1.4 IEEE 802.1x	46
4.3.2 Confirm Save Screen	47
4.4 The Profile Screen	48
4.4.1 Adding a New Profile	50
4.5 The Adapter Screen	54
Chapter 5	
Access Point Mode Configuration.....	57
5.1 Access Point Mode Introduction	57
5.1.1 ZyXEL Utility Screen Summary	57
5.1.2 Additional Setup Requirements	58
5.2 The Link Info Screen	58
5.3 The Configuration Screen	59
5.4 The MAC Filter Screen	61
Chapter 6	
Maintenance	63
6.1 The About Screen	63
6.2 Uninstalling the ZyXEL Utility	63
6.3 Upgrading the ZyXEL Utility	64
Chapter 7	
Troubleshooting	67
7.1 Problems Starting the ZyXEL Utility	67
7.2 Problem Connecting to an Access Point	67

7.3 Problem with the Link Quality	68
7.4 Problems Communicating With Other Computers	68

Appendix A	
Product Specifications	69

Appendix B	
Access Point Mode Setup Example	71

Appendix C	
Management with Wireless Zero Configuration	75

Appendix D	
Wireless Security	87

Appendix E	
Setting up Your Computer's IP Address	93

Index	99
--------------------	-----------

List of Figures

Figure 1 Application: Infrastructure	20
Figure 2 Application: Ad-Hoc	20
Figure 3 Application: Access Point Mode	21
Figure 4 ZyXEL Utility: Change Modes	21
Figure 5 ZyXEL Utility: System Tray Icon	22
Figure 6 Enable WZC	23
Figure 7 Infrastructure Network	25
Figure 8 ZyXEL Utility: Site Survey	26
Figure 9 ZyXEL Utility: Security Settings	26
Figure 10 ZyXEL Utility: Confirm Save	27
Figure 11 ZyXEL Utility: Link Info	27
Figure 12 ZyXEL Utility: Profile	28
Figure 13 ZyXEL Utility: Add New Profile	28
Figure 14 ZyXEL Utility: Profile Security	29
Figure 15 ZyXEL Utility: Profile Encryption	29
Figure 16 ZyXEL Utility: Wireless Frequency Settings	29
Figure 17 ZyXEL Utility: Profile Confirm Save	30
Figure 18 ZyXEL Utility: Profile Activate	30
Figure 19 ZyXEL Utility: AP: Link Info	31
Figure 20 ZyXEL Utility: AP: Configuration	32
Figure 21 Example of a Wireless Network	33
Figure 22 ZyXEL Utility Menu Summary: Station Mode	39
Figure 23 Station Mode: Link Info	40
Figure 24 Station Mode: Link Info: Trend Chart	41
Figure 25 Station Mode: Site Survey	42
Figure 26 Station Mode: Security Setting: WEP	43
Figure 27 Station Mode: Security Setting: WPA-PSK/WPA2-PSK	44
Figure 28 Station Mode: Security Settings: WPA/WPA2	45
Figure 29 Station Mode: Security Setting: 802.1x	46
Figure 30 Confirm Save Screen	48
Figure 31 Station Mode: Profile	49
Figure 32 Station Mode: Profile: Add a New Profile	50
Figure 33 Station Mode: Profile: Select Wireless Mode and Channel	51
Figure 34 Station Mode: Profile: Wireless Settings	52
Figure 35 Station Mode: Profile: Security Settings	53
Figure 36 Station Mode: Profile: Confirm New Settings	54
Figure 37 Station Mode: Profile: Activate the Profile	54
Figure 38 Station Mode: Adapter	55

Figure 39 ZyXEL Utility Menu Summary: AP Mode	57
Figure 40 Access Point Mode: Link Info	58
Figure 41 Access Point Mode: Configuration	59
Figure 42 Access Point Mode: MAC Filter	62
Figure 43 About	63
Figure 44 Uninstall: Confirm	64
Figure 45 Uninstall: Finish	64
Figure 46 Windows 2000: Start	71
Figure 47 Windows 2000: Network and Dial-up Connections	72
Figure 48 Windows 2000: Network Properties	72
Figure 49 WIndows 2000: Network Properties: Select Network Adapter	73
Figure 50 Windows 2000: Local Network	73
Figure 51 Windows XP SP2: WZC Not Available	75
Figure 52 Windows XP SP2: System Tray Icon	76
Figure 53 Windows XP SP2: Wireless Network Connection Status	76
Figure 54 Windows XP SP1: Wireless Network Connection Status	77
Figure 55 Windows XP SP2: Wireless Network Connection	77
Figure 56 Windows XP SP1: Wireless Network Connection Properties	78
Figure 57 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK ..	79
Figure 58 Windows XP SP2: Wireless Network Connection: No Security	79
Figure 59 Windows XP: Wireless (network) properties: Association	80
Figure 60 Windows XP: Wireless (network) properties: Authentication	81
Figure 61 Windows XP: Protected EAP Properties	82
Figure 62 Windows XP: Smart Card or other Certificate Properties	83
Figure 63 Windows XP SP2: Wireless Networks: Preferred Networks	84
Figure 64 Windows XP SP1: Wireless Networks: Preferred Networks	85
Figure 65 WPA-PSK Authentication	91
Figure 66 WPA(2) with RADIUS Application Example	92
Figure 67 Windows XP: Start Menu	93
Figure 68 Windows XP: Control Panel	94
Figure 69 Windows XP: Control Panel: Network Connections: Properties	94
Figure 70 Windows XP: Local Area Connection Properties	95
Figure 71 Windows XP: Advanced TCP/IP Settings	96
Figure 72 Windows XP: Internet Protocol (TCP/IP) Properties	97

List of Tables

Table 1 ZyXEL Utility: System Tray Icon	22
Table 2 ZyXEL Utility Menu Summary: Station Mode	39
Table 3 Station Mode: Link Info	40
Table 4 Station Mode: Link Info: Trend Chart	41
Table 5 Station Mode: Site Survey	42
Table 6 Station Mode: Security Setting: WEP	43
Table 7 Station Mode: Security Setting: WPA-PSK/WPA2-PSK	45
Table 8 Station Mode: Security Setting: WPA/WPA2	45
Table 9 Station Mode: Security Settings: IEEE 802.1x	47
Table 10 Confirm Save Screen	48
Table 11 Station Mode: Profile	49
Table 12 Station Mode: Profile: Add a New Profile	50
Table 13 Station Mode: Profile: Select a Channel	52
Table 14 Station Mode: Adapter	55
Table 15 ZyXEL Utility Menu Summary: AP Mode	57
Table 16 Access Point Mode: Link Info	58
Table 17 Access Point Mode: Configuration	60
Table 18 Access Point Mode: MAC Filter	62
Table 19 About	63
Table 20 Troubleshooting Starting ZyXEL Utility	67
Table 21 Troubleshooting Access Point Connection Problem	67
Table 22 Troubleshooting Link Quality	68
Table 23 Troubleshooting Communication Problem	68
Table 24 Product Specifications	69
Table 25 Windows XP SP2: System Tray Icon	76
Table 26 Windows XP SP2: Wireless Network Connection	78
Table 27 Windows XP: Wireless Networks	79
Table 28 Windows XP: Wireless (network) properties: Association	80
Table 29 Windows XP: Wireless (network) properties: Authentication	81
Table 30 Windows XP: Protected EAP Properties	82
Table 31 Windows XP: Smart Card or other Certificate Properties	83
Table 32 Comparison of EAP Authentication Types	89
Table 33 Wireless Security Relational Matrix	92

Preface

Congratulations on your purchase of the ZyXEL AG-225H v2 802.11a/g Wi-Fi Finder & Wireless USB Adapter. Your AG-225H v2 allows you to locate and access wireless networks.

Your AG-225H v2 is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your AG-225H v2 for its various applications.

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains hardware installation/connection information.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.








User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choice.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The ZyXEL AG-225H v2 802.11a/g Wi-Fi Finder & Wireless USB Adapter may be referred to as the AG-225H v2 in this user’s guide.

Graphics Icons Key

Wireless Access Point 	Computer 	Notebook Computer 
Server 	Modem or Router 	Wireless Signal 
Internet Cloud 		

CHAPTER 1

Getting Started

This chapter introduces the AG-225H v2 and prepares you to use the ZyXEL utility.

1.1 About Your AG-225H v2

The AG-225H v2 is an IEEE 802.11a/b/g compliant wireless LAN adapter that connects to the USB port on your computer and allows you to search for and connect to wireless networks. You can also turn your AG-225H v2 into an access point (AP) using the ZyXEL utility. The ZyXEL utility is a tool that helps you configure your AG-225H v2. See the appendix for detailed product specifications.

When the AG-225H v2 is not connected to a computer, you can locate wireless networks and see their details on the AG-225H v2's LCD screen. For more information about using the AG-225H v2 when it is not connected to a computer, see the Quick Start Guide.

1.2 Application Overview

This section describes some network applications for the AG-225H v2.

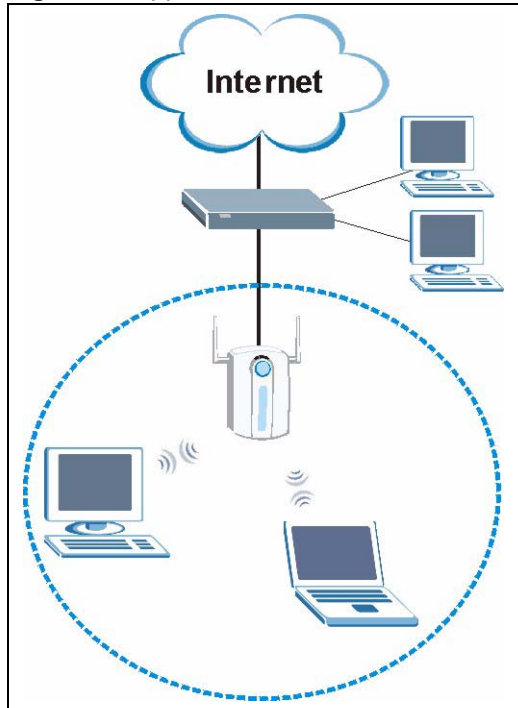
1.2.1 Station Mode

The AG-225H v2 is in wireless station mode by default. When the AG-225H v2 works as a wireless station (wireless client), you can either set the network type to **Infrastructure** and connect to an AP or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

1.2.1.1 Infrastructure

To connect to a network via an access point (AP), set the AG-225H v2 network type to **Infrastructure**. Through the AP, you can access the Internet or the wired network behind the AP.

Figure 1 Application: Infrastructure

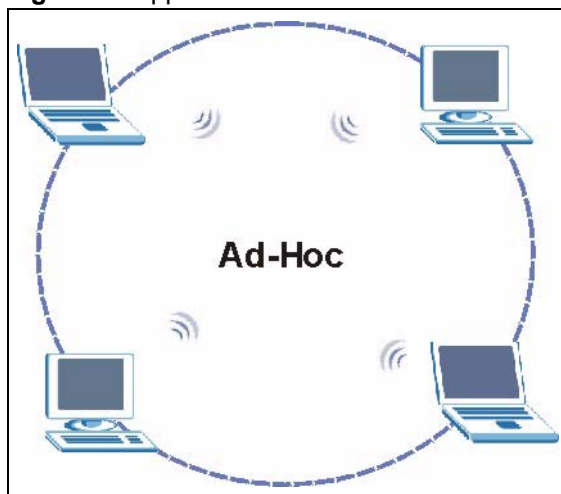


1.2.1.2 Ad-Hoc

To set up a small independent wireless workgroup without an AP, use **Ad-Hoc**.

Ad-Hoc does not require an AP or a wired network. Two or more wireless clients communicate directly with each other.

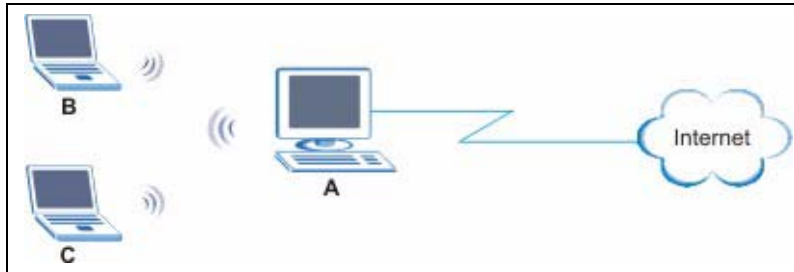
Figure 2 Application: Ad-Hoc



1.2.2 Access Point Mode

You can also set the AG-225H v2 to access point mode. This allows you to set up your wireless networks without using a dedicated AP. The following figure shows a network example.

Figure 3 Application: Access Point Mode

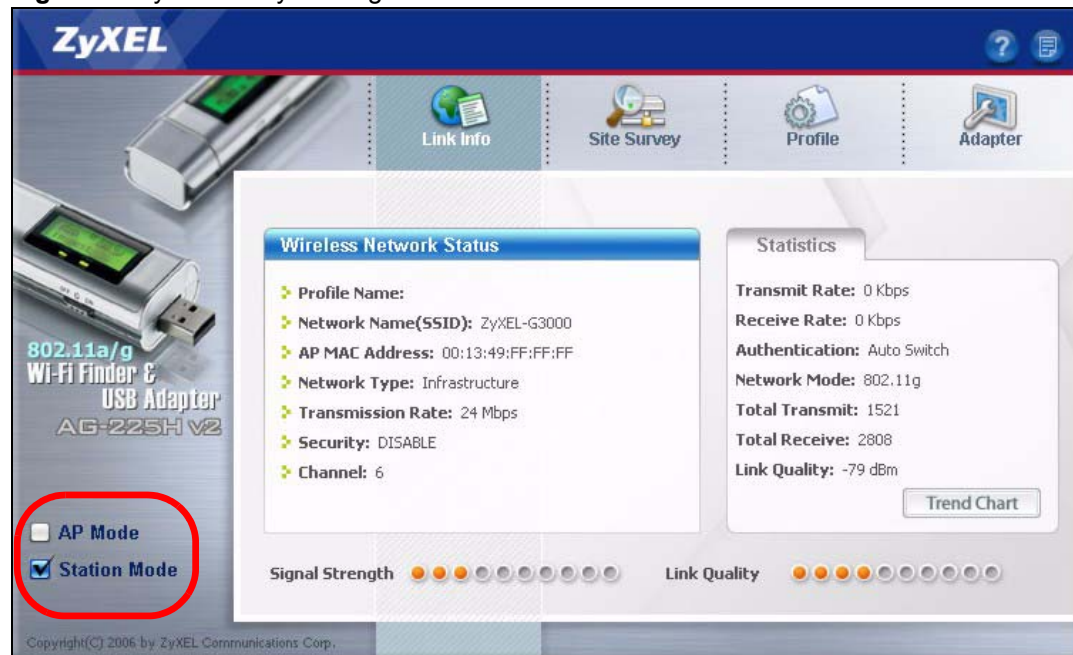


In the example, the AG-225H v2 is installed on computer **A** and set to operate in access point mode. Computer **A** provides an Internet connection to the wireless LAN, so wireless stations **B** and **C** can access the Internet.

1.2.3 Changing AG-225H v2 Mode

To change between the modes, select either **Station Mode** or **AP Mode** in any ZyXEL utility screens.

Figure 4 ZyXEL Utility: Change Modes



Note: Wait for about five seconds for the ZyXEL utility to complete the mode change. The current mode is indicated by the color of the check box.

1.3 AG-225H v2 Hardware and Utility Installation

Follow the instructions in the Quick Start Guide to install the ZyXEL utility and make hardware connections.

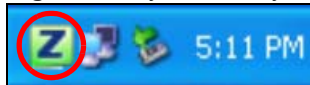
1.3.1 ZyXEL Utility Icon

After you install and start the ZyXEL utility, an icon for the ZyXEL utility appears in the system tray.

Note: The ZyXEL utility system tray icon displays only when the AG-225H v2 is installed properly.

When you use the ZyXEL utility, it automatically disables Wireless Zero Configuration (WZC).

Figure 5 ZyXEL Utility: System Tray Icon



The color of the ZyXEL utility system tray icon indicates the status of the AG-225H v2. Refer to the following table for details.

Table 1 ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The AG-225H v2 is operating in wireless station mode but is not connected to a wireless network.
Green	The AG-225H v2 is operating in wireless station mode and is connected to a wireless network.
Pale Blue	The AG-225H v2 is operating in access point mode.

1.4 Configuration Methods

To configure your AG-225H v2, use one of the following applications:

- Wireless Zero Configuration (WZC) (the Windows XP wireless configuration tool)
- ZyXEL Utility (required when you want to use the AG-225H v2 as an access point)

1.4.1 Enabling WZC

Note: When you use the ZyXEL utility, it automatically disables WZC.


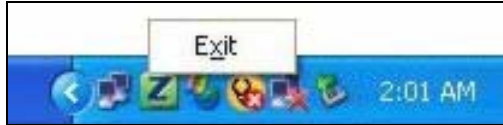

If you want to use WZC to configure the AG-225H v2, you need to disable the ZyXEL utility by right-clicking the utility icon () in the system tray and selecting **Exit**.

Figure 6 Enable WZC


Refer to the appendices for information on how to use WZC to manage the AG-225H v2.

To re-activate the ZyXEL utility, double-click the () icon on your desktop or click **Start, (All) Programs, ZyXEL AG-225H v2 Wireless Adapter Utility, ZyXEL AG-225H v2 Wireless Adapter Software.**

1.4.2 Accessing the ZyXEL Utility

Double-click on the ZyXEL wireless LAN utility icon in the system tray to open the ZyXEL utility.

The ZyXEL utility screens are similar in all Microsoft Windows versions. Screens for Windows XP are shown in this User's Guide.

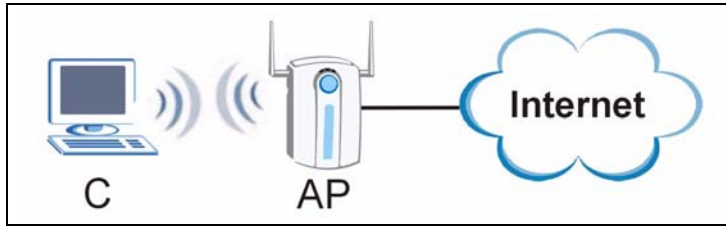
Note: Click the  icon (located in the top right corner) to display the online help window.

CHAPTER 2

Tutorial

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagrams. The wireless client is labeled **C** and the access point is labeled **AP**.

Figure 7 Infrastructure Network



There are three ways to connect the wireless client (the AG-225H v2 in station mode) to a network.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network (see [Section 2.1 on page 25](#)).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see [Section 2.2 on page 27](#)).

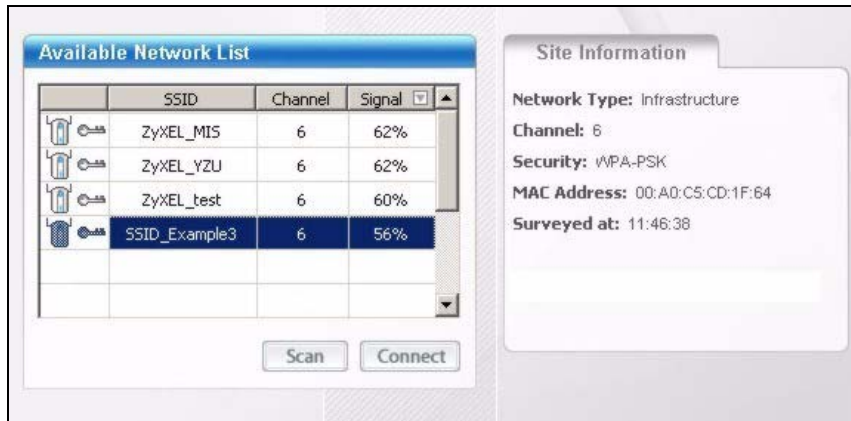
This chapter also includes a simple example of how to configure the AG-225H v2 as an AP using the ZyXEL utility. See [Section 2.3 on page 31](#) for more information.

2.1 Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set Identity (SSID) and WPA-PSK pre-shared key. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

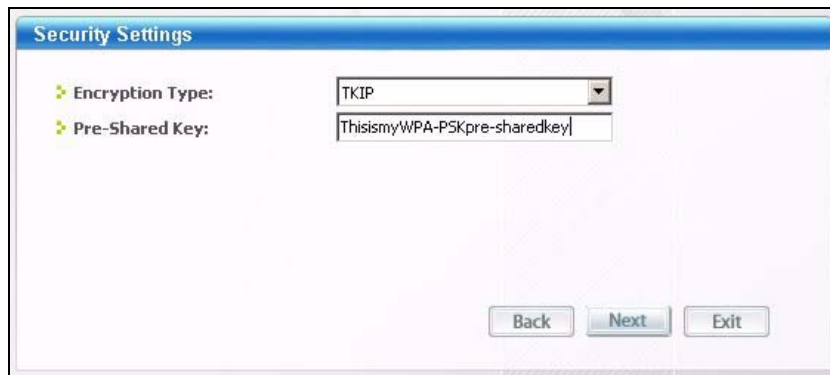
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

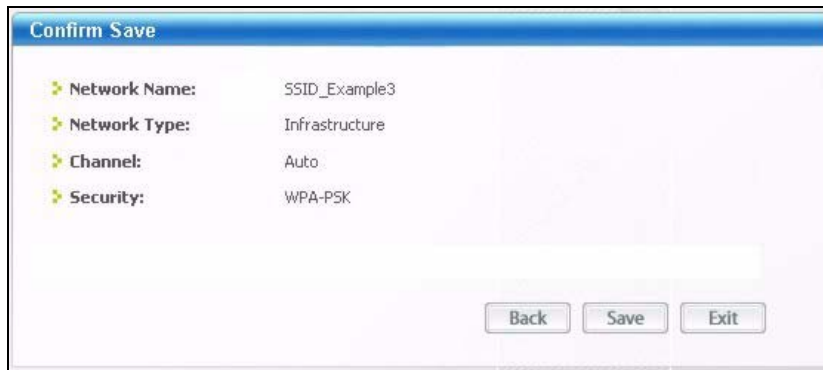
Figure 8 ZyXEL Utility: Site Survey

- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See [Table 5 on page 42](#) for detailed field descriptions.
- 3 To connect to an AP or peer computer, either click an entry in the list and then click **Connect** or double-click an entry (**SSID_Example3** in this example).
- 4 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

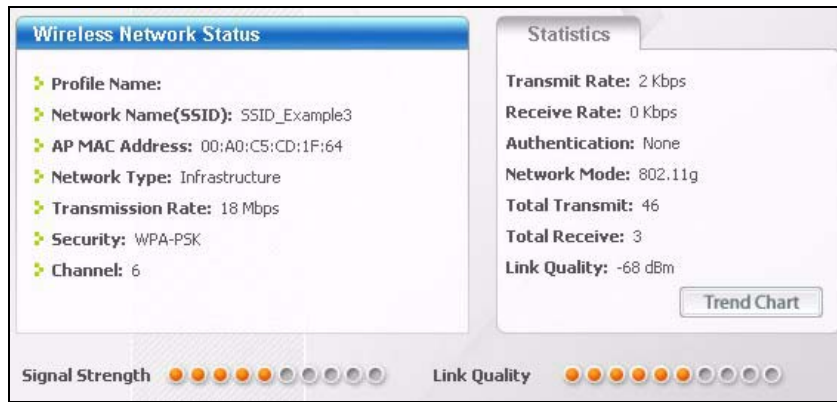
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 9 ZyXEL Utility: Security Settings

- 5 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 10 ZyXEL Utility: Confirm Save

- 6** The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank. See [Table 3 on page 40](#) for detailed field descriptions.

Figure 11 ZyXEL Utility: Link Info

- 7** Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured. If you cannot access the web site, check the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

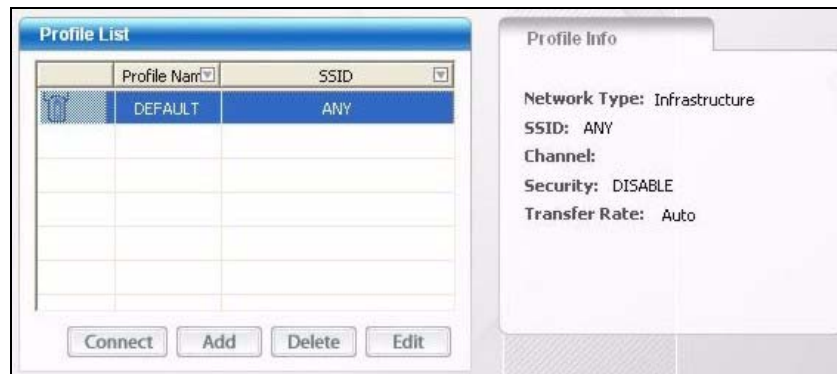
2.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the ZyXEL utility. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

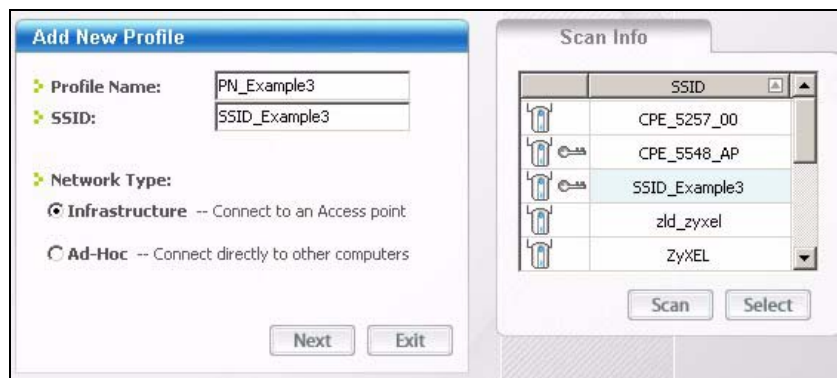
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen as shown. Click **Add** to configure a new profile.

Figure 12 ZyXEL Utility: Profile

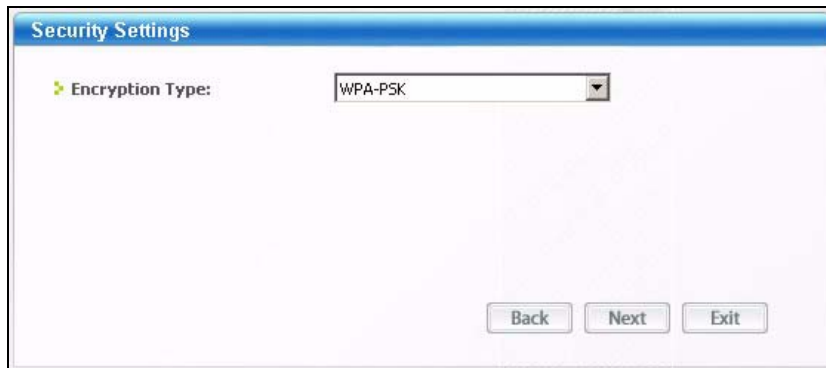


- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. You can also configure your profile for a wireless network that is not in the list.

Figure 13 ZyXEL Utility: Add New Profile



- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.
- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

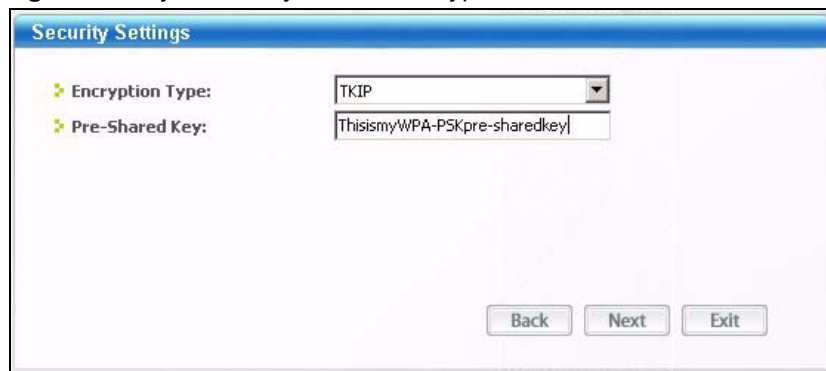
Figure 14 ZyXEL Utility: Profile Security

Security Settings

Encryption Type: WPA-PSK

Back Next Exit

- 5 This screen varies depending on the encryption method you selected in the previous screen. In this example, enter the pre-shared key and leave the encryption type at the default setting.

Figure 15 ZyXEL Utility: Profile Encryption

Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

Back Next Exit

- 6 In the next screen you can select which radio frequency to use. The **2.4GHz** frequency allows you to connect to a network using IEEE 802.11b or g only, and the **5GHz** frequency allows you to connect to a network using IEEE 802.11a only.

Leave both boxes checked to connect to a network using either IEEE 802.11a, b or g and click **Next**.

Figure 16 ZyXEL Utility: Wireless Frequency Settings

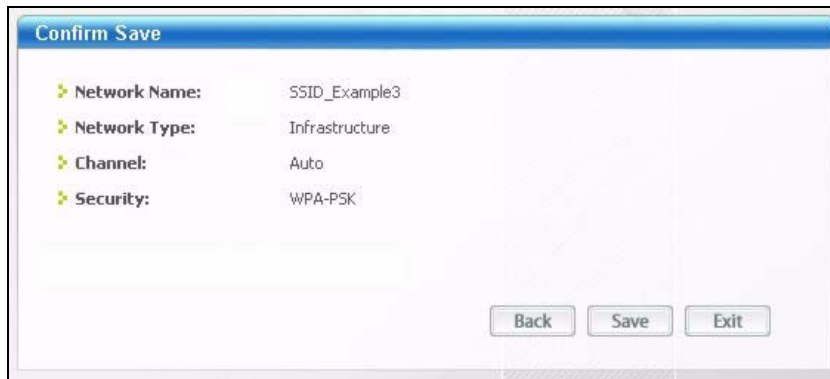
Wireless Protocol Settings

2.4 GHz

5 GHz

Back Next Exit

- 7 Verify the profile settings in the ready-only screen. Click **Save** to save and go to the next screen.

Figure 17 ZyXEL Utility: Profile Confirm Save

- 8** Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button to go back to the **Profile List** screen.

If you clicked **Activate Later** you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 18 ZyXEL Utility: Profile Activate

- 9** When you activate the new profile, the ZyXEL utility goes to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 10** Make sure the selected AP in the active profile is on and connected to the Internet. Open your Internet browser, enter <http://www.zyxel.com> or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.
- 11** If you cannot access the Internet, go back to the **Profile** screen. Select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

2.3 Configuring the AG-225H v2 as an AP

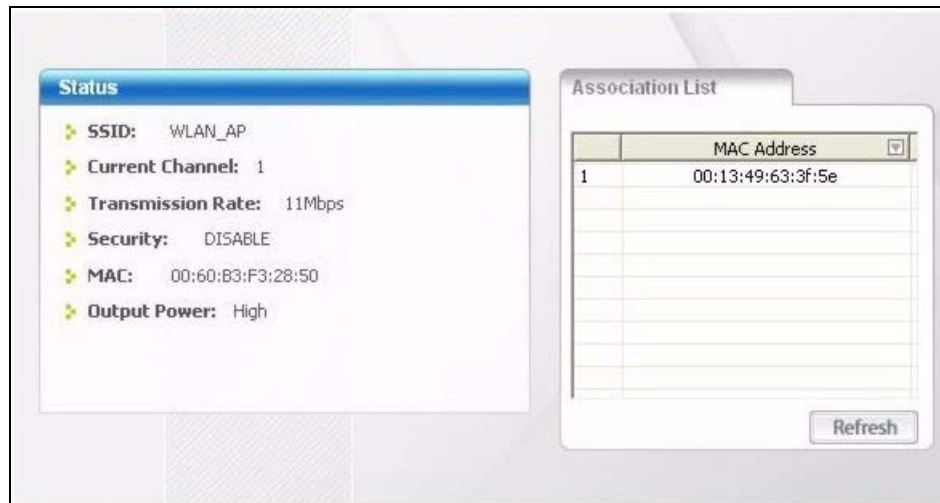
In access point mode, your AG-225H v2 allows you to set up your wireless network without using a dedicated AP. Refer to [Section 1.2.3 on page 21](#) and [Chapter 5 on page 57](#) for more information.

Note: With WZC, you cannot use the AG-225H v2 as an access point.

After you install the ZyXEL utility and then insert the AG-225H v2, follow the steps below to set up your AG-225H v2 as an AP.

- 1 Select **AP Mode** in any utility screen and wait for five seconds. The screen changes and displays as follows. Under **Status**, you can view the current settings on the AG-225H v2. In the **Association List**, you can see if any wireless clients have connected to your AG-225H v2.

Figure 19 ZyXEL Utility: AP: Link Info



- 2 If you want to change the SSID and enable wireless security for your AG-225H v2, click the **Configuration** tab and refer to [Section 5.3 on page 59](#) for detailed field descriptions.

Note: Only WEP security is available when the AG-225H v2 is in AP mode

Figure 20 ZyXEL Utility: AP: Configuration

The image shows a configuration dialog box for a ZyXEL AP, divided into two main sections: Wireless Settings and Security Settings. At the bottom right, there are 'Save' and 'Cancel' buttons.

Section	Setting	Value
Wireless Settings	SSID	WLAN_AP
	Hide SSID	<input type="checkbox"/>
	Wireless Mode	802.11b + 802.11g
	Channel	1
	Output Power	High
Security Settings	WEP	128 bits
	Authentication Type	Open
	Pass Phrase	
	Transmit Key	1
	Key 1	

CHAPTER 3

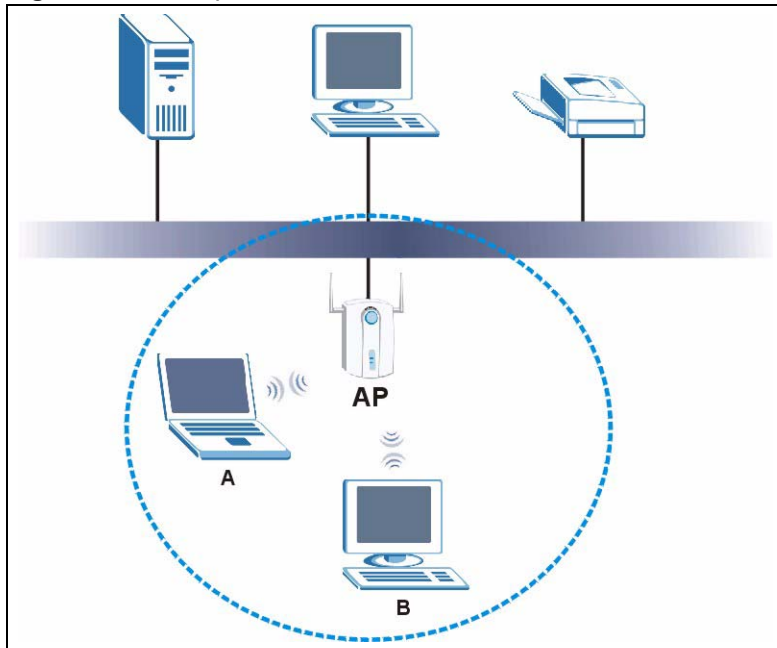
Wireless LAN Network

This chapter provides background information on wireless LAN networks.

3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See [Figure 2](#) on [page 20](#) for an Ad Hoc network example.

Figure 21 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP or peer computer.

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

3.2 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communications.

Configure the wireless LAN security using the **Configuration** or the **Profile Security Setting** screen. If you do not enable any wireless security on your AG-225H v2, the AG-225H v2's wireless communications are accessible to any wireless networking device that is in the coverage area.

Note: You can only use WEP encryption if you set the AG-225H v2 to Ad-hoc or AP mode.

See the appendices for more detailed information about wireless security.

3.2.1 Hide SSID

Normally, the AG-225H v2 in AP mode acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AG-225H v2 in AP mode does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

3.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the AG-225H v2 in AP mode which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

-
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to access the wireless network.

3.2.3 User Authentication and Encryption

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

3.2.3.1 WEP

3.2.3.1.1 Data Encryption

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AG-225H v2 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your AG-225H v2.

- Automatic WEP key generation based on a “password phrase” called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.

For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the ZyXEL utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

Your AG-225H v2 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys and only one key is used as the default key at any one time.

3.2.3.1.2 Authentication Type

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Two authentication types are defined: **Open** and **Shared**.

- Open mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

- Shared mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

3.2.3.2 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

3.2.3.2.1 EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. The AG-225H v2 supports EAP-TLS, EAP-TTLS and EAP-PEAP. Refer to [Appendix D on page 87](#) for descriptions.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

3.2.3.3 WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

CHAPTER 4

Wireless Station Mode Configuration

This chapter shows you how to configure your AG-225H v2 in wireless station mode. See [Chapter 5 on page 57](#) for how to configure the AG-225H v2 in access point mode.

4.1 Wireless Station Mode Overview

To set your AG-225H v2 to wireless station mode, select **Station Mode** in any utility screen (refer to [Section 1.2.3 on page 21](#)).

4.1.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens when the AG-225H v2 is in station mode.

Figure 22 ZyXEL Utility Menu Summary: Station Mode



The following table describes the menus.

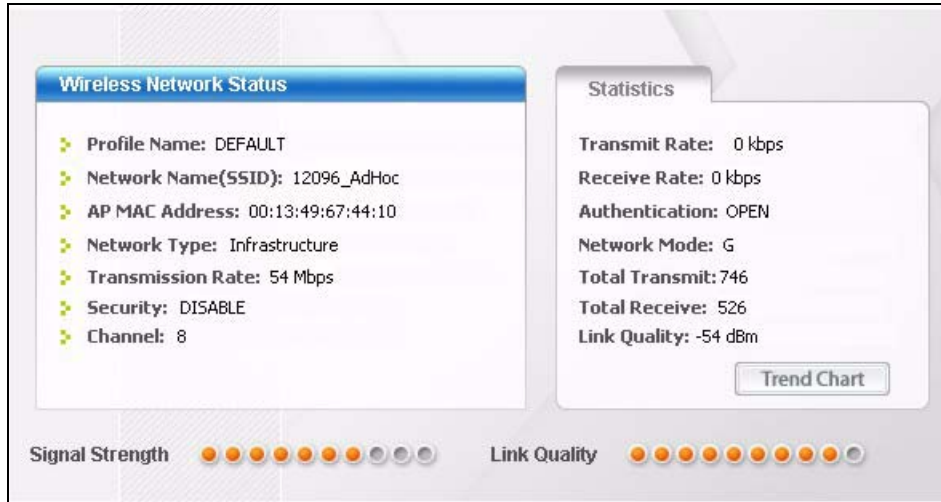
Table 2 ZyXEL Utility Menu Summary: Station Mode

TAB	DESCRIPTION
Station Mode	
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Site Survey	Use this screen to <ul style="list-style-type: none"> scan for a wireless network configure wireless security (if activated on the selected network). connect to a wireless network.
Profile	Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings.
Adapter	Use this screen to configure a transfer rate and enable power saving.

4.2 The Link Info Screen

When the ZyXEL utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your AG-225H v2.

Figure 23 Station Mode: Link Info



The following table describes the labels in this screen.

Table 3 Station Mode: Link Info

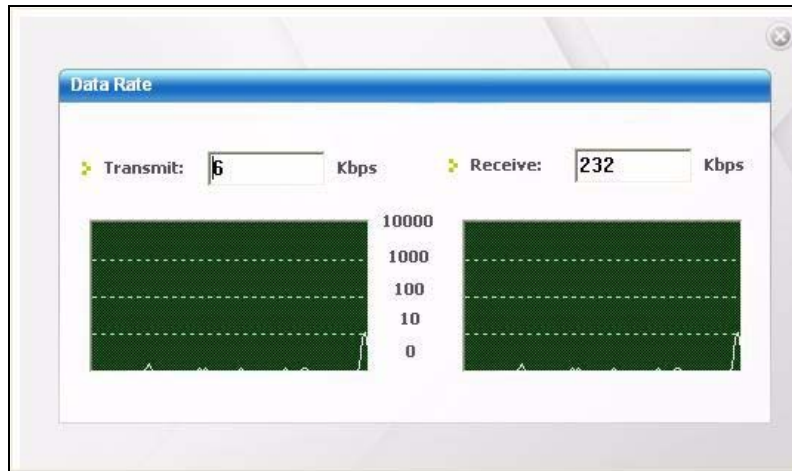
LABEL	DESCRIPTION
AP Mode Station Mode	Use the check box to set the AG-225H v2 to operate in wireless station or access point mode. Refer to Section 1.2.3 on page 21 for more information.
Wireless Network Status	
Profile Name	This is the name of the profile you are currently using.
Network Name (SSID)	The SSID identifies the wireless network to which a wireless station is associated. This field displays the name of the wireless device to which the AG-225H v2 is associated.
AP MAC Address	This field displays the MAC address of the AP or peer computer to which the AG-225H v2 is associated.
Network Type	This field displays the network type (Infrastructure or Ad-Hoc) of the wireless network.
Transmission Rate	This field displays the current transmission rate of the AG-225H v2 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (WEP, 802.1x, TKIP (WPA/WPA-PSK/WPA2/WPA2-PSK), AES (WPA/WPA-PSK/WPA2/WPA2-PSK)) or inactive (DISABLE).
Channel	This field displays the radio channel the AG-225H v2 is currently using.
Statistics	
Transmit Rate	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive Rate	This field displays the current data receiving rate in kilobits per second (Kbps).

Table 3 Station Mode: Link Info (continued)

LABEL	DESCRIPTION
Authentication	This field displays the authentication method of the AG-225H v2.
Network Mode	This field displays the wireless standard (A , B or G) of the AP or peer computer.
Total Transmit	This field displays the total number of data frames transmitted.
Total Receive	This field displays the total number of data frames received.
Link Quality	This field displays the signal strength of the AG-225H v2.
Trend Chart	Click this button to display the real-time statistics of the data rate in kilobits per second (Kbps).
Signal Strength	The status bar shows the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your AG-225H v2 and the AP or peer computer.
Link Quality	The status bar shows the quality of wireless connection. This refers to the percentage of packets transmitted successfully. If there are too many wireless stations in a wireless network, collisions may occur which could result in a loss of messages even though you have high signal strength.

4.2.1 Trend Chart

Click **Trend Chart** in the **Link Info** screen to display a screen as shown below. Use this screen to view real-time data traffic statistics.

Figure 24 Station Mode: Link Info: Trend Chart

The following table describes the labels in this screen.

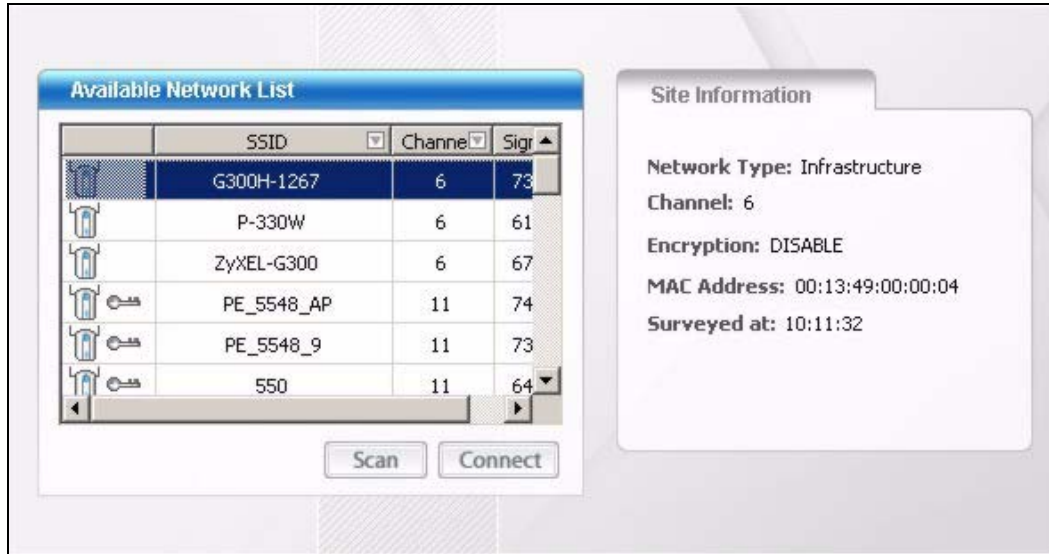
Table 4 Station Mode: Link Info: Trend Chart

LABEL	DESCRIPTION
Transmit	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive	This field displays the current data receiving rate in kilobits per second (Kbps).

4.3 The Site Survey Screen

Use the **Site Survey** screen to scan for and connect to a wireless network automatically.

Figure 25 Station Mode: Site Survey



The following table describes the labels in this screen.

Table 5 Station Mode: Site Survey










LABEL	DESCRIPTION
Available Network List	Click a column heading to sort the entries.
	 denotes that the wireless device is in infrastructure mode and the wireless security is activated.
	 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.
 or 	 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.
	 denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
SSID	This field displays the SSID (Service Set Identifier) of each wireless device.
Channel	This field displays the channel number used by each wireless device.
Signal	This field displays the signal strength of each wireless device.
Scan	Click Scan to search for available wireless devices within transmission range.
Connect	Click Connect to associate to the selected wireless device.
Site Information	Click an entry in the Available Network List table to display the information of the selected wireless device.
Network Type	This field displays the network type (Infrastructure or Ad Hoc) of the wireless device.
Channel	This field displays the channel number used by each wireless device.

Table 5 Station Mode: Site Survey (continued)

LABEL	DESCRIPTION
Encryption	This field shows whether data encryption is activated (WEP (WEP or 802.1x), WPA , WPA-PSK , WPA2 , WPA2-PSK) or inactive (DISABLE).
MAC address	This field displays the MAC address of the wireless device.
Surveyed at	This field displays the time when the wireless device was scanned.

4.3.1 Security Settings

When you configure the AG-225H v2 to connect to a network with wireless security activated and the security settings are disabled on the AG-225H v2, the screen varies according to the encryption method used by the selected network.

4.3.1.1 WEP Encryption

Figure 26 Station Mode: Security Setting: WEP

The screenshot shows a window titled "Security Settings" with the following fields and controls:

- WEP:** A dropdown menu set to "64 bits".
- Authentication Type:** A dropdown menu set to "Open".
- Pass Phrase:** An empty text input field.
- Transmit Key:** A dropdown menu set to "1".
- Key 1:** An empty text input field.

At the bottom of the window, there are three buttons: "Back", "Next", and "Exit".

The following table describes the labels in this screen.

Table 6 Station Mode: Security Setting: WEP

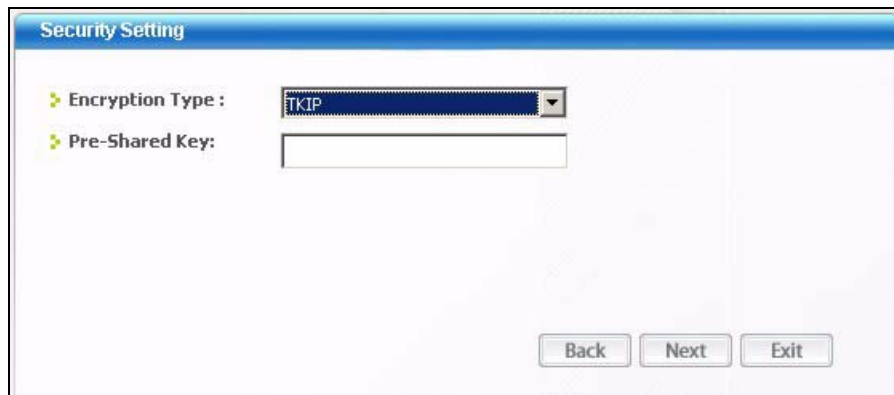
LABEL	DESCRIPTION
Security Settings	
WEP	Select 64 Bits , 128 Bits or 256 Bits to activate WEP encryption and then fill in the related fields.
Authentication Type	Select an authentication method. Choices are Open or Shared . Refer to Section 3.2.3.1.2 on page 35 for more information.
Pass Phrase	Enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the AG-225H v2 automatically generates four different WEP keys and displays it in the key field below. Refer to Section 3.2.3.1.1 on page 35 for more information. At the time of writing, you cannot use the passphrase function to generate 256-bit WEP keys.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.

Table 6 Station Mode: Security Setting: WEP (continued)

LABEL	DESCRIPTION
Key x (where x is a number between 1 and 4)	Select this option if you want to manually enter the WEP keys. Enter the WEP key in the field provided. If you select 64 Bits in the WEP field. Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type. or Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type. If you select 128 Bits in the WEP field, Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type or Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type. If you select 256 Bits in the WEP field, Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type or Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey1111222233334444555566678) for ASCII key type. Note: The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive.
Back	Click Back to go to the Site Survey screen to select and connect to another network.
Next	Click Next to confirm your selections and advance to the Confirm Save screen. Refer to Section 4.3.2 on page 47 .
Exit	Click Exit to return to the Site Survey screen without saving.

4.3.1.2 WPA-PSK/WPA2-PSK

Figure 27 Station Mode: Security Setting: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 7 Station Mode: Security Setting: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (TKIP or AES) for data encryption. Refer to Section 3.2.3.2.1 on page 36 for more information.
Pre-Shared Key	Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Back	Click Back to go to the Site Survey screen to select and connect to another network.
Next	Click Next to confirm your selections and advance to the Confirm Save screen. Refer to Section 4.3.2 on page 47 .
Exit	Click Exit to return to the Site Survey screen without saving.

4.3.1.3 WPA/WPA2

Figure 28 Station Mode: Security Settings: WPA/WPA2

The screenshot shows a window titled "Security Settings" with the following fields and controls:

- Encryption Type:** A dropdown menu with "AES" selected.
- Authentication Type:** A dropdown menu with "PEAP" selected.
- Login Name:** An empty text input field.
- Password:** An empty text input field.
- Server CA:** A dropdown menu with "<Trust Any>" selected.
- PEAP Inner EAP:** A dropdown menu with "MS CHAP V2" selected.

At the bottom of the window, there are three buttons: "Back", "Next", and "Exit".

The following table describes the labels in this screen.

Table 8 Station Mode: Security Setting: WPA/WPA2

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (TKIP or AES) for data encryption. Refer to Section 3.2.3.2.1 on page 36 for more information.
Authentication Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are TLS and PEAP .
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.

Table 8 Station Mode: Security Setting: WPA/WPA2

LABEL	DESCRIPTION
Password	This field is not available when you select TLS in the Authentication Type field. Enter the password associated with the user name above.
Certificate	This field is only available when you select TLS in the Authentication Type field. Click Browse to select a certificate. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Server CA	Select a certificate authority (CA) from the drop-down box to have the AG-225H v2 trust certificates from that CA only. Select Trust Any to accept certificates from any CA.
PEAP Inner EAP	This field is only available when you select PEAP in the Authentication Type field. The PEAP method used by the RADIUS server or AP for client authentication is MS CHAP v2 .
Back	Click Back to go to the Site Survey screen to select and connect to another network.
Next	Click Next to confirm your selections and advance to the Confirm Save screen. Refer to Section 4.3.2 on page 47 .
Exit	Click Exit to return to the Site Survey screen without saving.

4.3.1.4 IEEE 802.1x

Configure IEEE 802.1x security with various authentication methods in this screen.

Figure 29 Station Mode: Security Setting: 802.1x



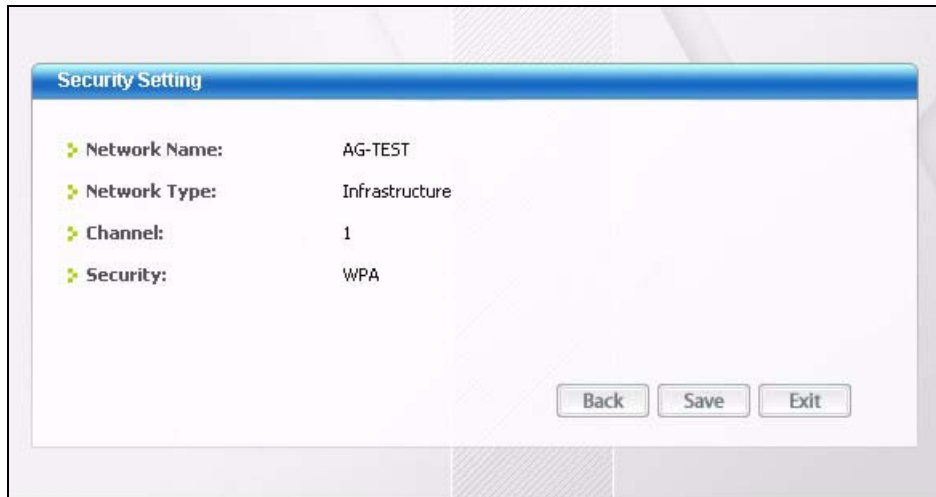
The following table describes the labels in this screen.

Table 9 Station Mode: Security Settings: IEEE 802.1x

LABEL	DESCRIPTION
Authentication Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are TLS and PEAP .
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select TLS in the Authentication Type field. Enter the password associated with the user name above.
Certificate	This field is only available when you select TLS in the Authentication Type field. Click Browse to select a certificate. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Server CA	Select a certificate authority (CA) from the drop-down box to have the AG-225H v2 trust certificates from that CA only. Select Trust Any to accept certificates from any CA.
PEAP Inner EAP	This field is only available when you select PEAP in the Authentication Type field. The PEAP method used by the RADIUS server or AP for client authentication is MS CHAP v2 .
Back	Click Back to go to the Site Survey screen to select and connect to another network.
Next	Click Next to confirm your selections and advance to the Confirm Save screen. Refer to Section 4.3.2 on page 47 .
Exit	Click Exit to return to the Site Survey screen without saving.

4.3.2 Confirm Save Screen

Use this screen to confirm and save the security settings.

Figure 30 Confirm Save Screen

The following table describes the labels in this screen.

Table 10 Confirm Save Screen

LABEL	DESCRIPTION
Security Setting	
Network Name	This field displays the SSID previously entered.
Network Type	This field displays the network type (Infrastructure or Ad-Hoc) of the wireless device.
Channel	This field displays the channel number used by the profile.
Security	This field shows whether data encryption is activated (WEP (WEP or 802.1x), WPA , WPA-PSK , WPA2 , WPA2-PSK) or inactive (DISABLE).
Back	Click Back to return to the previous screen.
Save	Click Save to save the changes to the AG-225H v2 and display the Link Info screen.
Exit	Click Exit to discard changes and return to the Site Survey screen.

4.4 The Profile Screen

A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the AG-225H v2, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the AG-225H v2 cannot connect to a network.

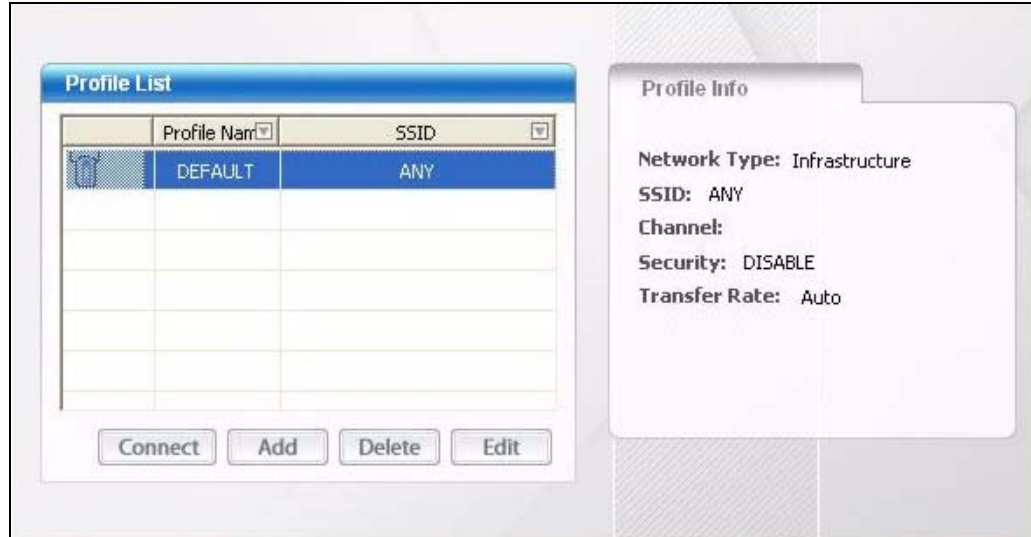
If you do not configure and activate a profile, each time you start the AG-225H v2, the AG-225H v2 uses the default profile to connect to any available network that has no security enabled.

The default profile is a profile that allows you to connect to any SSID that has no security enabled.

Click the **Profile** tab in the ZyXEL utility program to display the **Profile** screen as shown next.

The profile function allows you to save the wireless network settings in this screen, or use one of the pre-configured network profiles.

Figure 31 Station Mode: Profile



The following table describes the labels in this screen.

Table 11 Station Mode: Profile









LABEL	DESCRIPTION
Profile List	Click a column heading to sort the entries.
 ,	 denotes that the wireless device is in infrastructure mode and the wireless security is activated.
 ,	 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.
 or	 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.
 .	 denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
Profile Name	This is the name of the pre-configured profile.
SSID	This is the SSID of the wireless network to which the selected profile associate.
Connect	To use and activate a previously saved network profile, select a pre-configured profile name in the table and click Connect .
Add	To add a new profile into the table, click Add .
Delete	To delete an existing wireless network configuration, select a profile in the table and click Delete .
Edit	To edit an existing wireless network configuration, select a profile in the table and click Edit .
Profile Info	The following fields display detailed information of the selected profile in the Profile List table.
Network Type	This field displays the network type (Infrastructure or Ad-Hoc) of the profile.

Table 11 Station Mode: Profile (continued)

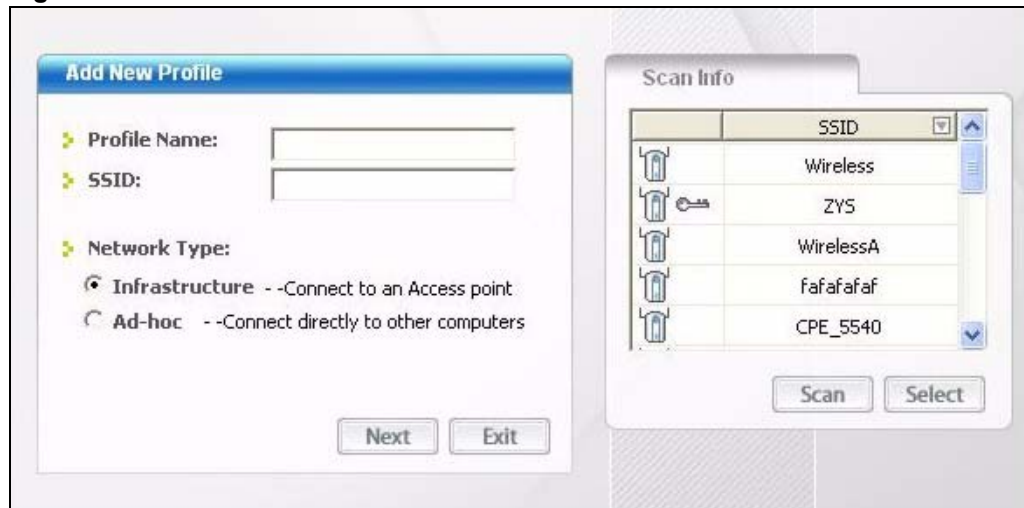
LABEL	DESCRIPTION
SSID	This field displays the SSID (Service Set Identifier) of the profile.
Channel	This field displays the channel number used by the profile.
Security	This field shows whether data encryption is activated (WEP, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1x) or inactive (DISABLE).
Transfer Rate	This field displays the transmission speed of the selected profile in megabits per second (Mbps).

4.4.1 Adding a New Profile

Follow the steps below to add a new profile.

- 1 Click **Add** in the **Profile** screen. An **Add New Profile** screen displays as shown next. Click **Next** to continue.

Figure 32 Station Mode: Profile: Add a New Profile











The following table describes the labels in this screen.

Table 12 Station Mode: Profile: Add a New Profile

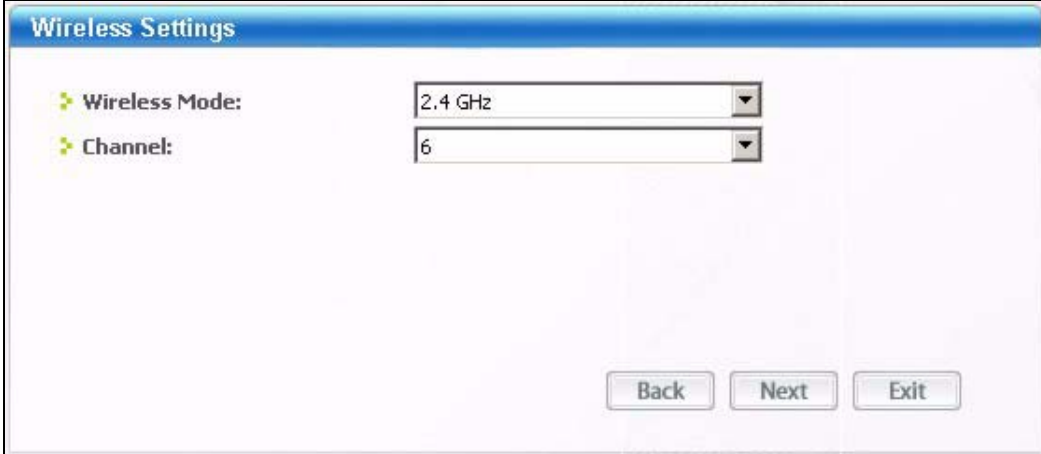
LABEL	DESCRIPTION
Add New Profile	
Profile Name	Enter a descriptive name in this field.
SSID	Select an available wireless device in the Scan Info table and click Select , or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter Any to have the AG-225H v2 associate to any AP or roam between any infrastructure wireless networks.
Network Type	Select Infrastructure to associate to an AP. Select Ad-Hoc to associate to a peer computer.
Next	Click Next to go to the next screen.
Exit	Click Exit to go back to the previous screen without saving.

Table 12 Station Mode: Profile: Add a New Profile (continued)

LABEL	DESCRIPTION
Scan Info	This table displays the information of the available wireless networks within the transmission range.
 ,	 denotes that the wireless device is in infrastructure mode and the wireless security is activated.
 ,	 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.
 or	 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.
 .	 denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
SSID	This field displays the SSID (Service Set Identifier) of each AP or peer device.
Scan	Click Scan to search for available wireless devices within transmission range.
Select	Select an available wireless device in the table and click Select to add it to this profile. Whenever you activate this profile, the AG-225H v2 associates to the selected wireless network only.

- 2** If you select the **Infrastructure** network type in the previous screen, skip to step 3. If you select the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a wireless frequency and channel number and click **Next** to continue.

Note: To associate to an ad-hoc network, you must use the same channel and wireless frequency as the peer computer.

Figure 33 Station Mode: Profile: Select Wireless Mode and Channel


The screenshot shows a window titled "Wireless Settings". It contains two expandable sections, each with a green arrow icon to its left. The first section is "Wireless Mode:" and its dropdown menu is currently set to "2.4 GHz". The second section is "Channel:" and its dropdown menu is currently set to "6". At the bottom right of the window, there are three buttons: "Back", "Next", and "Exit".

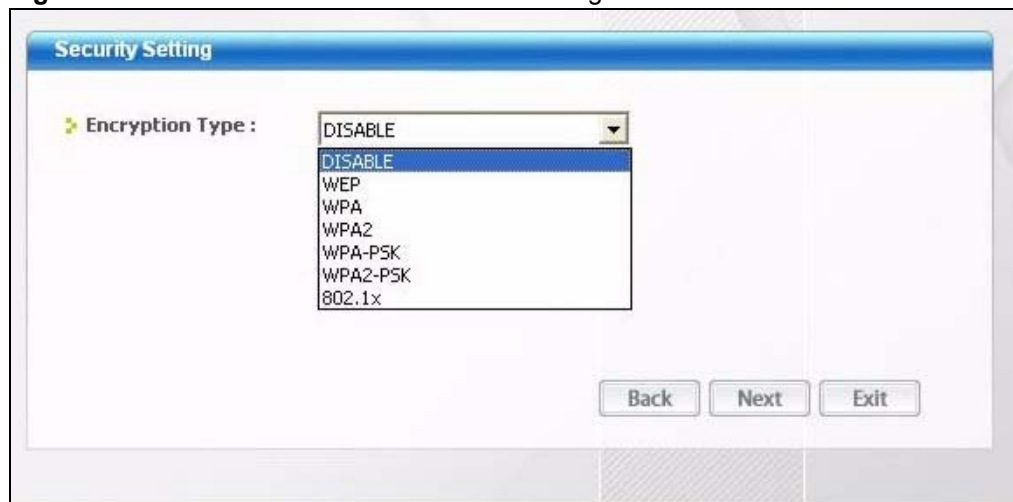
The following table describes the labels in this screen.

Table 13 Station Mode: Profile: Select a Channel

LABEL	DESCRIPTION
Wireless Settings	
Wireless Mode	Choose a wireless frequency: 2.4GHz or 5GHz . The 2.4GHz frequency is used by the IEEE 802.11b and IEEE 802.11g wireless standards, and the 5GHz frequency is used by the IEEE 802.11a wireless standard.
Channel	Select a channel number from the drop-down list box. To associate to an ad-hoc network, you must use the same channel as the peer computer.

- 3** If you selected **Infrastructure** network type in the first screen, select **WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK** or **802.1x** from the drop-down list box to enable data encryption. If you selected **Ad-Hoc** network type in the first screen, you can use only **WEP** encryption method. Otherwise, select **DISABLE** to allow the AG-225H v2 to communicate with the access points or other peer wireless computers without any data encryption, and skip to step **5**.

Figure 34 Station Mode: Profile: Wireless Settings

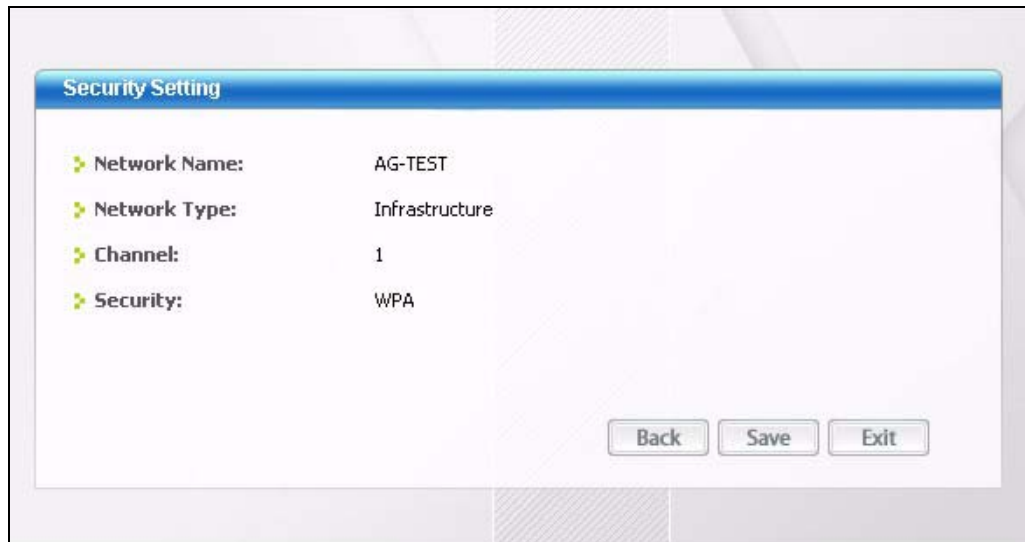


- 4** The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the APs or other peer wireless computers as they are on the AG-225H v2. Refer to [Section 4.3.1 on page 43](#) for detailed information on wireless security configuration.

Figure 35 Station Mode: Profile: Security Settings

- 5** If you selected the **Ad-Hoc** network type previously, skip to step **6**. If you selected the **Infrastructure** network type previously, a screen displays as follows. Choose which radio frequencies to set. If you select **2.4GHz** you will be able to communicate with wireless devices in IEEE 802.11b mode and IEEE 802.11g modes only, and if you select **5GHz** you will be able to communicate with wireless devices in IEEE 802.11a mode only. Leave both boxes checked to communicate with wireless devices in a, b and g modes.

- 6** This read-only screen shows a summary of the new profile settings. Verify that the settings are correct. Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen. Otherwise, click **Exit** to go back to the **Profile** screen without saving.

Figure 36 Station Mode: Profile: Confirm New Settings

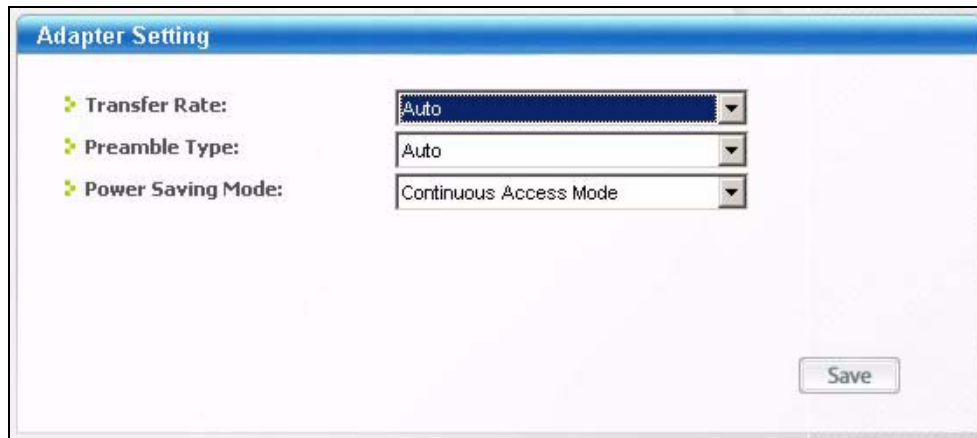
7 To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button. You can activate only one profile at a time.

Note: Once you activate a profile, the ZyXEL utility will use that profile the next time it is started.

Figure 37 Station Mode: Profile: Activate the Profile

4.5 The Adapter Screen

To set the other advanced features on the AG-225H v2, click the **Adapter** tab.

Figure 38 Station Mode: Adapter

The following table describes the labels in this screen.

Table 14 Station Mode: Adapter

LABEL	DESCRIPTION
Adapter Setting	
Transfer Rate	<p>In most networking scenarios, the factory default Auto setting is the most efficient and allows your AG-225H v2 to operate at the highest possible transmission (data) rate.</p> <p>If you want to select a specific transmission rate, select one that the AP or peer wireless device supports.</p> <p>Note: With USB1.0/1.1, the AG-225H v2 can only transmit at up to 11Mbps.</p>
Preamble Type	<p>Preamble is used to signal that data is coming to the receiver. Select the preamble type that the AP uses. Short and Long refer to the length of the synchronization field in a packet.</p> <p>Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support Long preamble, but not all support short preamble.</p> <p>Select Auto to have the AG-225H v2 automatically use short preamble when all access point or wireless stations support it; otherwise the AG-225H v2 uses long preamble.</p> <p>Note: The AG-225H v2 and the access point or wireless stations MUST use the same preamble mode in order to communicate.</p>
Power Saving Mode	<p>Select Maximum Power Save or Fast Power Save to save power (especially for notebook computers). This forces the AG-225H v2 to go to sleep mode when it is not transmitting data.</p> <p>When you select Continuous Access Mode, the AG-225H v2 will never go to sleep mode.</p>
Save	Click Save to save the changes to the AG-225H v2.

CHAPTER 5

Access Point Mode Configuration

This chapter shows you how to configure your AG-225H v2 in access point mode.

5.1 Access Point Mode Introduction

To set your AG-225H v2 to access point (AP) mode, select **AP Mode** in any utility screen (refer to [Section 1.2.3 on page 21](#)).

Access point mode allows you to set up your wireless networks without using a dedicated AP.

5.1.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens when the AG-225H v2 is in AP mode.

Figure 39 ZyXEL Utility Menu Summary: AP Mode



The following table describes the menu.

Table 15 ZyXEL Utility Menu Summary: AP Mode

TAB	DESCRIPTION
AP Mode	
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Configuration	Use this screen to configure wireless LAN settings.
MAC Filter	Use this screen to configure which computer(s) you want access to the wireless LAN through the AG-225H v2.

5.1.2 Additional Setup Requirements

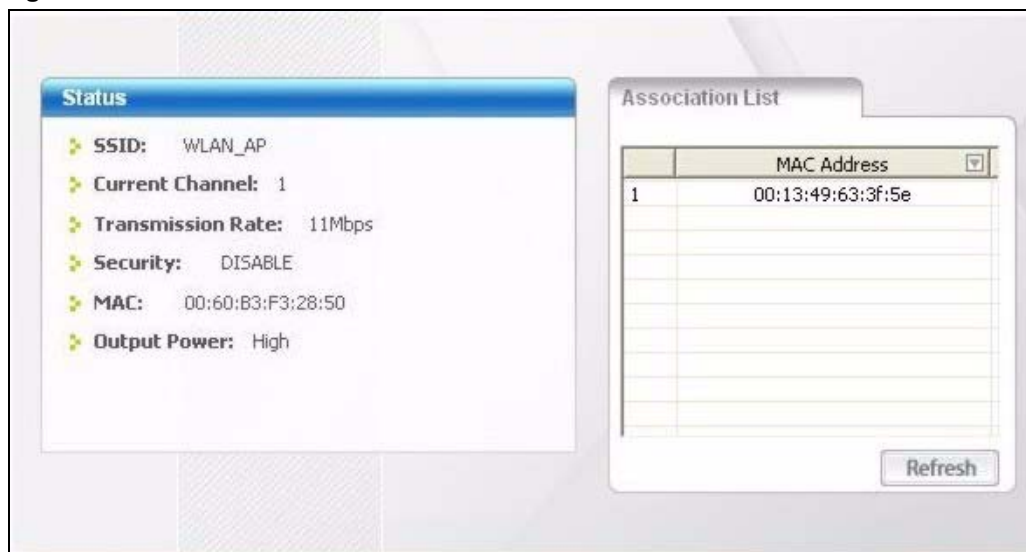
To bridge your wired and wireless network using the AG-225H v2, the following requirements must be met:

- 1 The AG-225H v2 must be installed on a computer connected to the wired network.
- 2 Either bridge the two interfaces (wireless and wired) on the computer (using the **Configuration** screen of the ZyXEL utility in Windows XP) or configure network sharing (refer to [Appendix B on page 71](#) for an example).
- 3 Set the wireless station's IP address to be dynamic if you want the wireless stations to access the wired network or the Internet through the AG-225H v2. Refer to [Appendix E on page 93](#) for how to configure your computer's IP address.

5.2 The Link Info Screen

Select the **AP Mode** check box and wait for about five seconds to display the screen as shown.

Figure 40 Access Point Mode: Link Info







The following table describes the labels in this screen.

Table 16 Access Point Mode: Link Info

LABEL	DESCRIPTION
Status	
SSID	This field displays the name that identifies your AG-225H v2 in the wireless LAN network.
Current Channel	This field displays the radio channel the AG-225H v2 is currently using.
Transmission Rate	This field displays the current transmission rate of the AG-225H v2 in megabits per second (Mbps).

Table 16 Access Point Mode: Link Info (continued)

LABEL	DESCRIPTION
Security	This field shows whether data encryption is activated (WEP) or inactive (DISABLE).
MAC	This field displays the MAC address of the AG-225H v2.
Output Power	This field shows the strength of the AG-225H v2's antenna gain or transmission power.
Association List	This table lists up to 16 wireless clients that are currently connected to the AG-225H v2.
 or	 denotes a wireless client without WEP security.
	 denotes a wireless client with WEP security enabled.
MAC Address	This field displays the MAC addresses of a wireless client that is currently connected to the AG-225H v2.
Refresh	Click Refresh to update this screen.

5.3 The Configuration Screen

Click **Configuration** in the ZyXEL utility screen to display the screen as shown.

Figure 41 Access Point Mode: Configuration


The screenshot displays two configuration panels side-by-side. The left panel, titled "Wireless Settings", includes fields for SSID (set to WLAN_AP), a checkbox for "Hide SSID", Wireless Mode (set to 802.11b + 802.11g), Channel (set to 1), and Output Power (set to High). The right panel, titled "Security Settings", includes fields for WEP (set to 128 bits), Authentication Type (set to Open), Pass Phrase (empty), Transmit Key (set to 1), and Key 1 (empty). At the bottom right of the configuration area are "Save" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 17 Access Point Mode: Configuration

LABEL	DESCRIPTION
Wireless Settings	
SSID	<p>The SSID identifies the wireless network to which a wireless station is associated. Wireless stations associating with the access point (the AG-225H v2) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p>
Hide SSID	<p>Select this check box to hide the SSID so an intruder cannot obtain the SSID through scanning using a site survey tool.</p>
Wireless Mode	<p>Set this field to allow wireless stations using different wireless modes to connect to the AP (the AG-225H v2).</p> <p>Select 802.11b + 802.11g (default) to allow wireless stations using both IEEE 802.11b and IEEE 802.11g modes to connect to the AP.</p> <p>Select 802.11b to allow only wireless clients using IEEE 802.11b mode to connect to the AP.</p> <p>Select 802.11g to allow only wireless clients using IEEE 802.11g mode to connect to the AP.</p> <p>Select 802.11a to allow only wireless clients using IEEE 802.11a mode to connect to the AP.</p>
Channel	<p>Set the operating frequency/channel depending on your geographical region.</p>
Output Power	<p>Set this field if you need to conserve power consumption (especially for notebook computers). This control changes the strength of the AG-225H v2's antenna gain or transmission power. Antenna gain, measured in dBm (decibel relative units compared to milliwatts), is the increase in coverage. Higher antenna gain improves the range of the signal for better communications.</p> <p>Select High to set the AG-225H v2's antenna to transmit at 17-dBm.</p> <p>Select Medium-High to set the AG-225H v2's antenna to transmit at 15-dBm.</p> <p>Select Medium-Low to set the AG-225H v2's antenna to transmit at 13-dBm.</p> <p>Select Low to set the AG-225H v2's antenna to transmit at 11-dBm. This allows for the least power consumption.</p>
Security Settings	
WEP	<p>Select 64 Bits, 128 Bits or 256 Bits to activate WEP encryption and then fill in the related fields.</p> <p>Select Disable to deactivate the WEP encryption.</p>
Authentication Type	<p>Select an authentication method. Choices are Shared and Open.</p> <p>Refer to Section 3.2.3.1.2 on page 35 for more information.</p>
Pass Phrase	<p>Enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the AG-225H v2 automatically generates four different WEP key and displays the first in the key field below. Refer to Section 3.2.3.1 on page 35 for more information.</p> <p>At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.</p>
Transmit Key	<p>Select a default WEP key to use for data encryption. The key displays in the field below.</p>

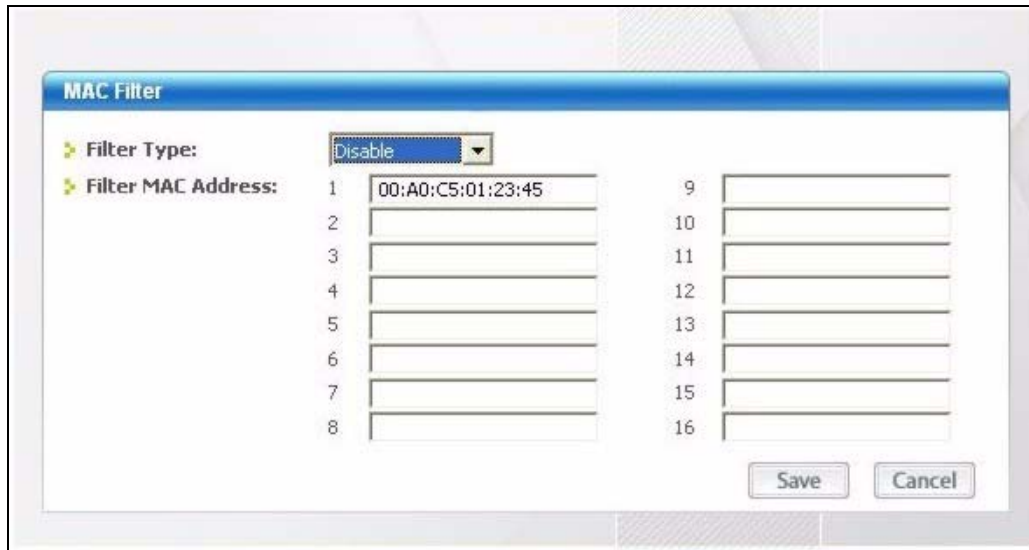
Table 17 Access Point Mode: Configuration (continued)

LABEL	DESCRIPTION
Key x (where x is a number between 1 and 4)	<p>Select this option if you want to manually enter the WEP keys.</p> <p>Enter the WEP key in the field provided.</p> <p>If you select 64 Bits in the WEP field.</p> <p>Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type</p> <p>or</p> <p>Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type.</p> <p>If you select 128 Bits in the WEP field,</p> <p>Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type</p> <p>or</p> <p>Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type.</p> <p>If you select 256 Bits in the WEP field,</p> <p>Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type</p> <p>or</p> <p>Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey111122223333444455556678) for ASCII key type.</p> <p>Note: The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN.</p> <p>ASCII WEP keys are case sensitive.</p>
Save	Click Save to save the changes.
Cancel	Click Cancel to discard the changes.

5.4 The MAC Filter Screen

The **MAC Filter** screen allows you to configure the AG-225H v2 to give exclusive access to devices (**Accept**) or exclude devices from connecting to the AG-225H v2 (**Reject**). The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the device(s) to configure this screen. See [Section 3.2.2 on page 34](#) for more information.

Figure 42 Access Point Mode: MAC Filter



The following table describes the labels in this screen.

Table 18 Access Point Mode: MAC Filter

LABEL	DESCRIPTION
Filter Type	Define the filter action for the list of MAC addresses in the MAC address filter table. Select Disable to deactivate the MAC filter feature. Select Reject to block access to the AG-225H v2. MAC addresses not listed will be allowed to access the AG-225H v2. Select Accept to permit access to the AG-225H v2. MAC addresses not listed will be denied access to the AG-225H v2.
Filter MAC Address 1-16	Specify the MAC address(es) of the wireless station(s) that is allowed or denied association to the AG-225H v2. Enter six pairs of hexadecimal digits (separated by colons) in the range of "A-F", "a-f" and "0-9" (for example, 00:A0:C5:00:00:02). If you enter an invalid MAC address, once you click Save to save the values, a warning screen will be displayed.
Save	Click Save to save the changes to the AG-225H v2.
Cancel	Click Cancel to discard the changes.

CHAPTER 6

Maintenance

This chapter describes how to uninstall or upgrade the ZyXEL utility.

6.1 The About Screen


The **About** screen displays driver and utility version numbers of the AG-225H v2. To display the screen shown below, click the about () button.

Figure 43 About



The following table describes the read-only fields in this screen.

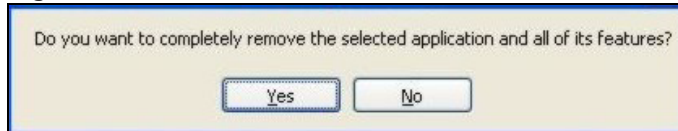
Table 19 About

LABEL	DESCRIPTION
Driver Version	This field displays the version number of the AG-225H v2 driver.
Utility Version	This field displays the version number of the ZyXEL utility.

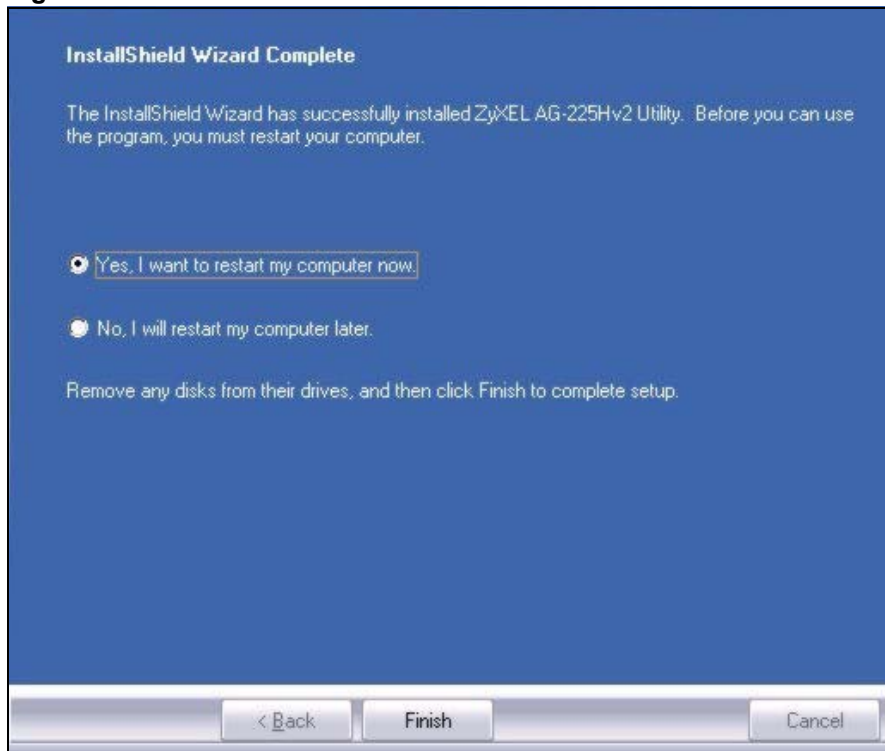
6.2 Uninstalling the ZyXEL Utility

Follow the steps below to remove (or uninstall) the ZyXEL utility from your computer.

- 1** Click **Start, (All) Programs, ZyXEL AG-225H v2 Wireless USB Adapter Utility, Uninstall ZyXEL AG-225H v2 Wireless USB Adapter Utility.**
- 2** When prompted, click **OK** or **Yes** to remove the driver and the utility software.

Figure 44 Uninstall: Confirm

- 3 Click **Finish** to complete uninstalling the software and restart the computer when prompted.

Figure 45 Uninstall: Finish

6.3 Upgrading the ZyXEL Utility

Note: Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

To perform the upgrade, follow the steps below.

- 1 Download the latest version of the utility from the ZyXEL web site and save the file on your computer.
- 2 Follow the steps in [Section 6.2 on page 63](#) to remove the current ZyXEL utility from your computer.
- 3 Restart your computer when prompted.
- 4 Disconnect the AG-225H v2 from your computer.
- 5 Double-click on the setup program for the new utility to start the ZyXEL utility installation.

- 6 Insert the AG-225H v2 and check the version numbers in the **About** screen to make sure the new utility is installed properly.

CHAPTER 7

Troubleshooting

This chapter covers potential problems and the possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

7.1 Problems Starting the ZyXEL Utility

Table 20 Troubleshooting Starting ZyXEL Utility

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyXEL Wireless LAN utility	<p>Make sure the AG-225H v2 is properly inserted and the LED is on. Refer to the Quick Start Guide for the LED descriptions.</p> <p>Use the Device Manager to check for possible hardware conflicts. Click Start, Settings, Control Panel, System, Hardware and Device Manager. Verify the status of the AG-225H v2 under Network Adapter. (Steps may vary depending on the version of Windows).</p> <p>Install the AG-225H v2 in another computer.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.</p>
The ZyXEL utility icon does not display.	If you have installed the Funk Odyssey Client software on the computer, uninstall (remove) both the Funk Odyssey Client software and ZyXEL utility, and then install the ZyXEL utility again after restarting the computer.

7.2 Problem Connecting to an Access Point

Table 21 Troubleshooting Access Point Connection Problem

PROBLEM	CORRECTIVE ACTION
When using the Windows XP configuration tool, the AG-225H v2 cannot scan for or connect to any access points.	<p>The AG-225H v2 might still be operating in access point mode. This results when you set the AG-225H v2 to operate in access point mode using the ZyXEL utility, close the ZyXEL utility and then use the Windows XP configuration tool.</p> <p>Before you use the Windows XP configuration tool, make sure you set the AG-225H v2 to operate in station mode before you close and exit the ZyXEL utility.</p>

7.3 Problem with the Link Quality

Table 22 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	<p>Search and connect to another AP with a better link quality using the Site Survey screen.</p> <p>Move your computer closer to the AP or the peer computer(s) within the transmission range.</p> <p>There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Lower the output power of each AP.</p> <p>Make sure there are not too many wireless stations connected to a wireless network.</p>

7.4 Problems Communicating With Other Computers

Table 23 Troubleshooting Communication Problem

PROBLEM	CORRECTIVE ACTION
In wireless station mode, the computer with the AG-225H v2 installed cannot communicate with the other computer(s).	<p>In Infrastructure Mode</p> <ul style="list-style-type: none"> • Make sure that the AP and the associated computers are turned on and working properly. • Make sure the AG-225H v2 computer and the associated AP use the same SSID. • Change the AP and the associated wireless clients to use another radio channel if interference is high. • Make sure that the computer and the AP share the same security option and key. Verify the settings in the Profile Security Setting screen. • If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa. <p>In Ad-Hoc (IBSS) Mode</p> <ul style="list-style-type: none"> • Verify that the peer computer(s) is turned on. • Make sure the AG-225H v2 computer and the peer computer(s) are using the same SSID and channel. • Make sure that the computer and the peer computer(s) share the same security settings. • Change the wireless clients to use another radio channel if interference is high.
In access point mode, the wireless station(s) cannot associate to the AG-225H v2.	<p>Verify that the computer with the AG-225H v2 installed is turned on.</p> <p>Make sure the wireless station(s) uses the same SSID as the AG-225H v2.</p> <p>Make sure the wireless station(s) uses the same security settings.</p> <p>Verify that the wireless station(s) is not blocked in the MAC Filter screen.</p>

APPENDIX A

Product Specifications

Table 24 Product Specifications

PHYSICAL AND ENVIRONMENTAL SPECIFICATIONS	
Product Name	ZyXEL AG-225H v2 802.11a/g Wi-Fi Finder & Wireless USB Adapter
Interface	USB 2.0 compatible
Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 60 degrees Centigrade
Operating Humidity	20 ~ 95% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Power	TX power consumption: < 380mA RX power consumption: < 200mA
Voltage	5V
Weight	36g
Dimensions	(W) 99 mm × (D) 32 mm × (H) 16 mm
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Operating Frequencies	IEEE 802.11a: North America: 5.15~5.850GHz Europe: 5.15~5.725GHz Taiwan: 5.15~5.850GHz IEEE 802.11b 2.4~2.4835GHz IEEE 802.11g: 2.4~2.4835GHz

Table 24 Product Specifications (continued)

Operating Channels	<p>IEEE 802.11a</p> <p>North America 5.15~5.25GHz: 4 5.25~5.35GHz: 4 5.725~5.850GHz: 5</p> <p>Europe 5.15~5.25GHz: 4 5.25~5.35GHz: 4 5.470~5.725GHz : 11</p> <p>Taiwan 5.15~5.25GHz : 4 5.25~5.35GHz: 3 5.725~5.850GHz: 5</p> <p>IEEE 802.11b North America: 11 Europe: 13 Taiwan: 11</p> <p>IEEE 802.11g: North America: 11 Europe: 13 Taiwan: 11</p>
Data Rate	<p>IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, 6 Mbps</p> <p>IEEE 802.11b: 11, 5.5, 2, 1Mbps</p> <p>IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps</p>
Modulation	<p>IEEE 802.11a: Orthogonal Frequency Division Multiplexing (OFDM)</p> <p>IEEE 802.11b: Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK).</p> <p>IEEE 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)</p>
Output Power	<p>IEEE 802.11a: 12dBm (+/- 2dBm) at 54Mbps, OFDM</p> <p>IEEE 802.11b: 17dBm (+/- 2dBm) at 11Mbps, CCK, QPSK, BPSK</p> <p>IEEE 802.11g: 14dBm (+/- 2dBm) at 54Mbps, OFDM</p>
RX Sensitivity	<p>IEEE 802.11g (OFDM): 54 Mbps: < -70 dBm</p> <p>IEEE 802.11b (CCK): 11 Mbps: < -85 dBm</p>
SOFTWARE SPECIFICATIONS	
Device Drivers	Windows 2000, Windows XP
Security	<p>64/128/256-bit WEP</p> <p>WPA/WPA-PSK/WPA2/WPA2-PSK</p> <p>IEEE 802.1x</p>
Roaming	IEEE 802.11b/g compliant

APPENDIX B

Access Point Mode Setup Example

This example uses the network sharing feature in Windows 2000 to bridge the wired and wireless network when you set the AG-225H v2 in access point (AP) mode.

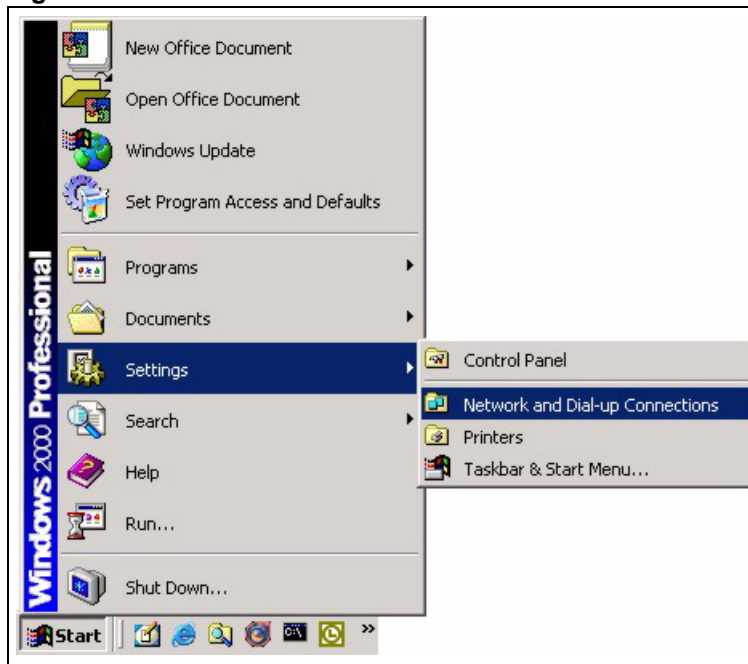
Refer to [Chapter 5 on page 57](#) for setup methods and requirements.

Steps may vary depending on your Windows version.

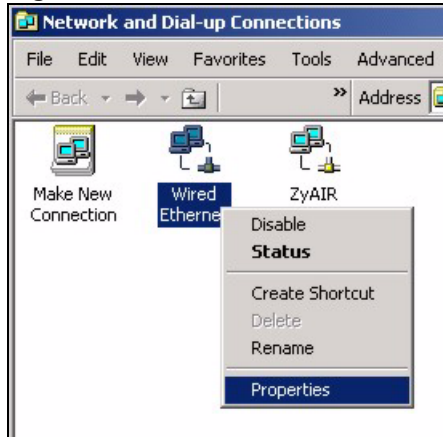
Configuring the Computer on Which You Install the AG-225H v2

- 1 Refer to [Section 1.2.3 on page 21](#) to set the AG-225H v2 to operate in AP mode.
- 2 Click **Start, Settings, Network and Dial-up Connections** (or click **Start, Settings, Control Panel** and double-click **Network and Dial-up Connections**).

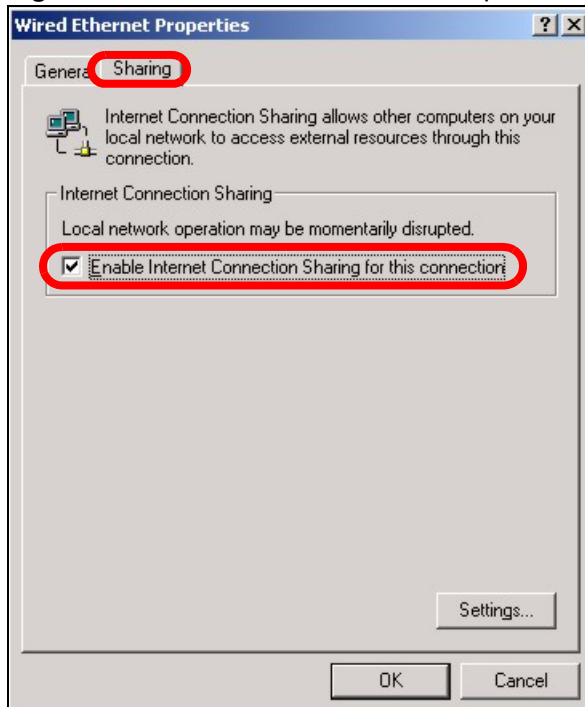
Figure 46 Windows 2000: Start



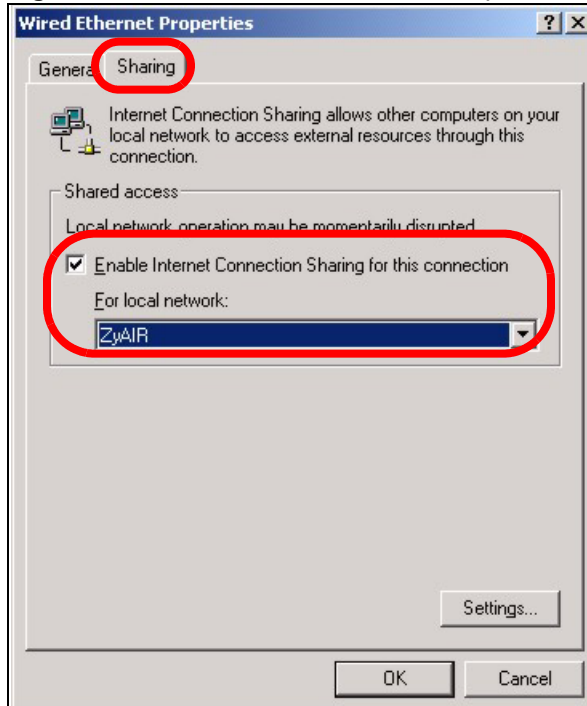
- 3 Right-click on the icon for your wired Ethernet adapter and click **Properties**.

Figure 47 Windows 2000: Network and Dial-up Connections

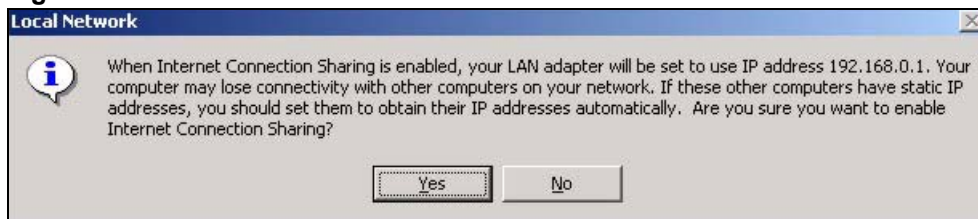
4 A **Properties** screen displays. Click the **Sharing** tab and select **Enable Internet Connection Sharing for this connection**. Click **OK**.

Figure 48 Windows 2000: Network Properties

If there is more than one network adapter on the computer, select **Enable Internet Connection Sharing for this connection** and select the network adapter to which you want to share network access.

Figure 49 Windows 2000: Network Properties: Select Network Adapter

5 A notice screen displays. Click **Yes**.

Figure 50 Windows 2000: Local Network

Configuring the Wireless Station Computer


Refer to [Appendix E on page 93](#) for information on how to set up the IP address of a computer you want to connect wirelessly to the AG-225H v2.

APPENDIX C

Management with Wireless Zero Configuration

This appendix shows you how to manage your AG-225H v2 using the Windows XP wireless zero configuration tool.

Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

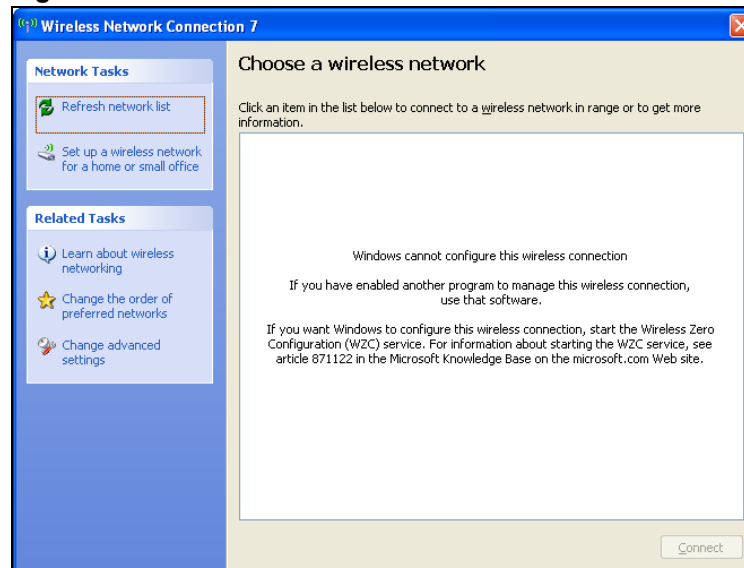
Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon () in most screens, move the cursor to the item that you want the information about and click to view the help.

Activating Wireless Zero Configuration

Make sure the **Use Windows to configure my wireless network settings** check box is selected in the **Wireless Network Connection Properties** screen. Refer to [Appendix C on page 71](#).

If you see the following screen, refer to article 871122 on the Microsoft web site for information on starting WZC.

Figure 51 Windows XP SP2: WZC Not Available



Connecting to a Wireless Network

- 1 Double-click the network icon for wireless connections in the system tray to open the Wireless Network Connection Status screen.

Figure 52 Windows XP SP2: System Tray Icon



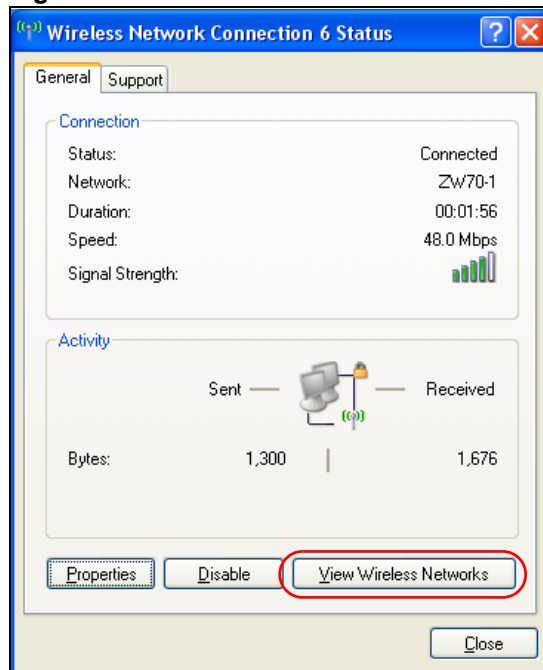
The type of the wireless network icon in Windows XP SP2 indicates the status of the AG-225H v2. Refer to the following table for details.

Table 25 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
	The AG-225H v2 is connected to a wireless network.
	The AG-225H v2 is in the process of connecting to a wireless network.
	The connection to a wireless network is limited because the network did not assign a network address to the computer.
	The AG-225H v2 is not connected to a wireless network.

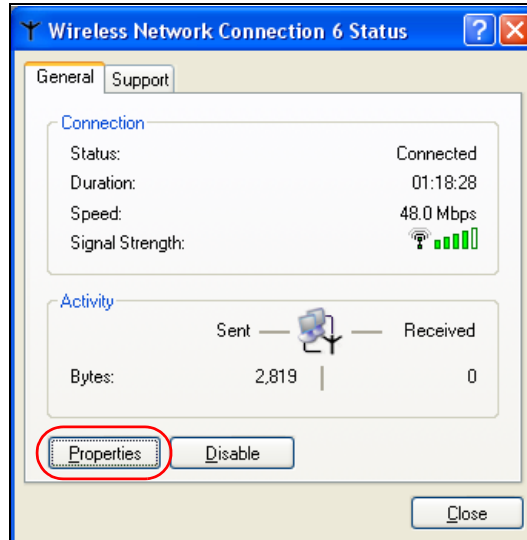
- 2 Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.

Figure 53 Windows XP SP2: Wireless Network Connection Status



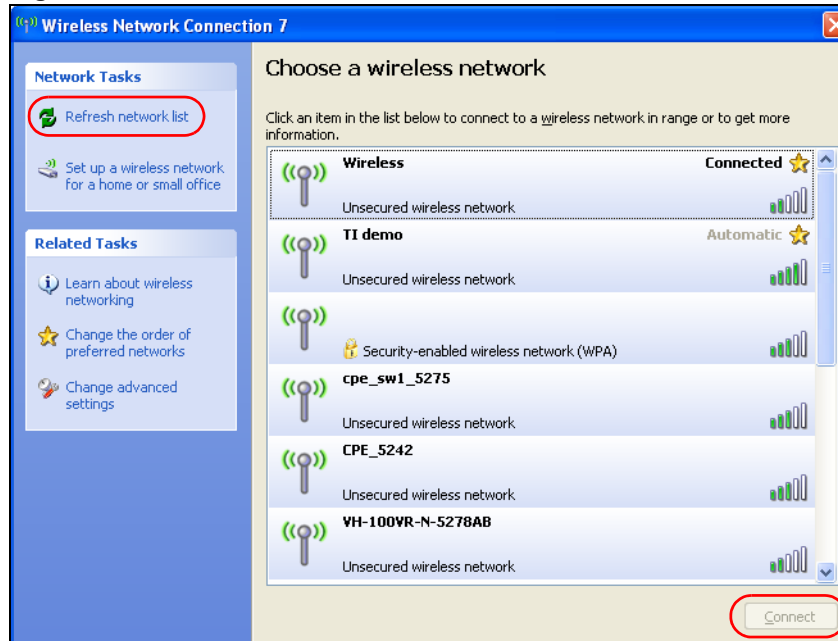
Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.

Figure 54 Windows XP SP1: Wireless Network Connection Status






- Windows XP SP2: Click **Refresh network list** to reload and search for available wireless devices within transmission range. Select a wireless network in the list and click **Connect** to join the selected wireless network.

Figure 55 Windows XP SP2: Wireless Network Connection



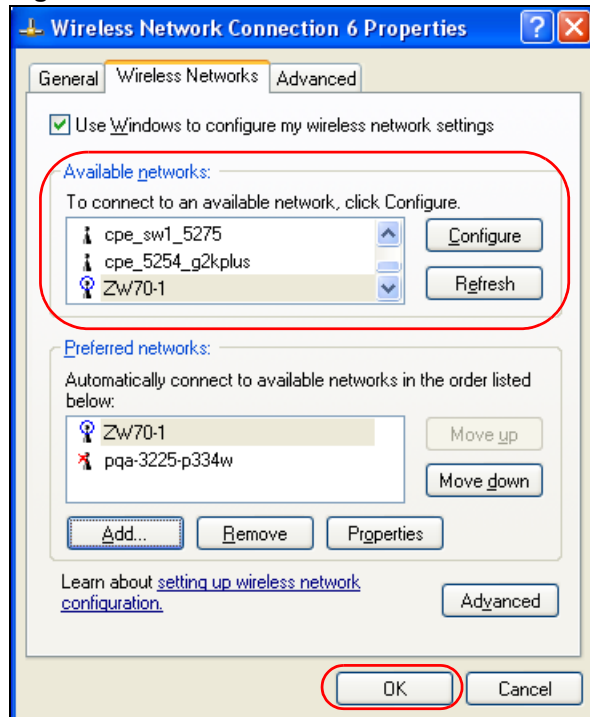
The following table describes the icons in the wireless network list.

Table 26 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
	This denotes that wireless security is activated for the wireless network.
	This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the AG-225H v2 tries to associate to the preferred network first in the order that you specify. Refer to the section on ordering the preferred networks for detailed information.
	This denotes the signal strength of the wireless network. Move your cursor to the icon to see details on the signal strength.

Windows XP SP1: Click **Refresh** to reload and search for available wireless devices within transmission range. Select a wireless network in the **Available networks** list, click **Configure** and set the related fields to the same security settings as the associated AP to add the selected network into the **Preferred** networks table. Click **OK** to join the selected wireless network. Refer to the section on security settings (discussed later) for more information.

Figure 56 Windows XP SP1: Wireless Network Connection Properties



4. Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP and click **Connect**. Refer to the section about security settings for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption.

If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.

Figure 57 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK

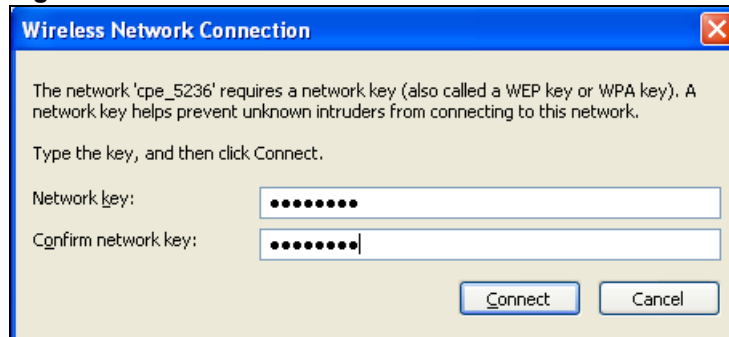
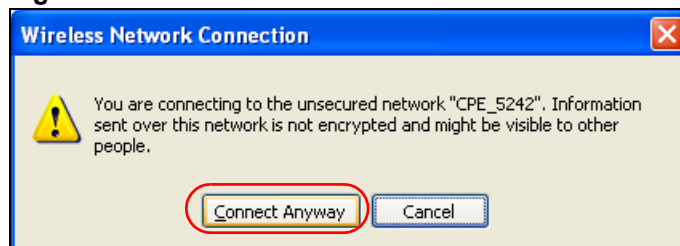


Figure 58 Windows XP SP2: Wireless Network Connection: No Security



- 5 Verify that you have successfully connected to the selected network and check the connection status in the wireless network list or the connection icon in the **Preferred networks** or **Available networks** list.

The following table describes the connection icons.

Table 27 Windows XP: Wireless Networks

ICON	DESCRIPTION
	This denotes the wireless network is an available wireless network.
	This denotes the AG-225H v2 is associated to the wireless network.
	This denotes the wireless network is not available.

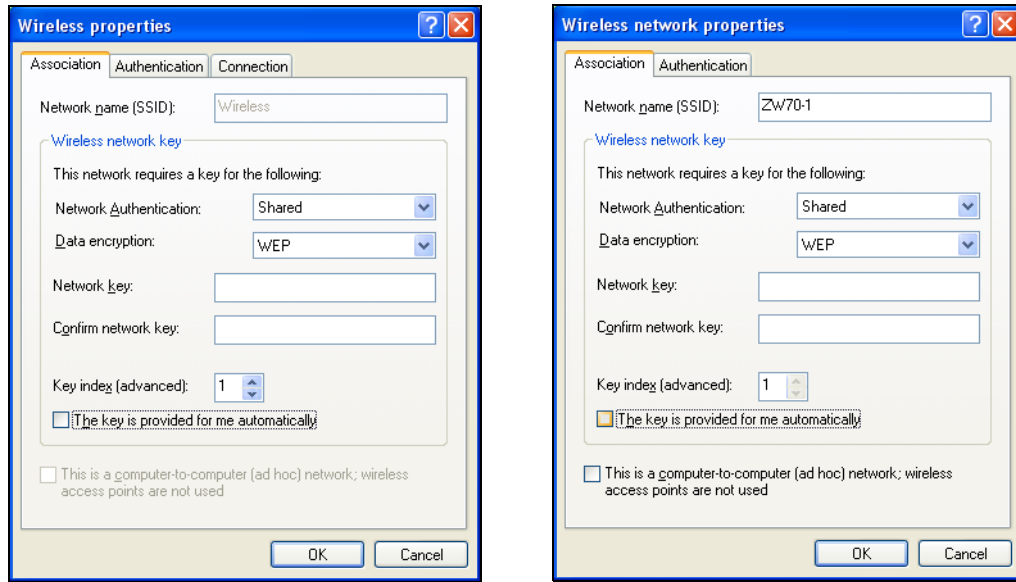
Security Settings

When you configure the AG-225H v2 to connect to a secure network but the security settings are not yet enabled on the AG-225H v2, you will see different screens according to the authentication and encryption methods used by the selected network.

Association

Select a network in the Preferred networks list and click Properties to view or configure security.

Figure 59 Windows XP: Wireless (network) properties: Association



The following table describes the labels in this screen.

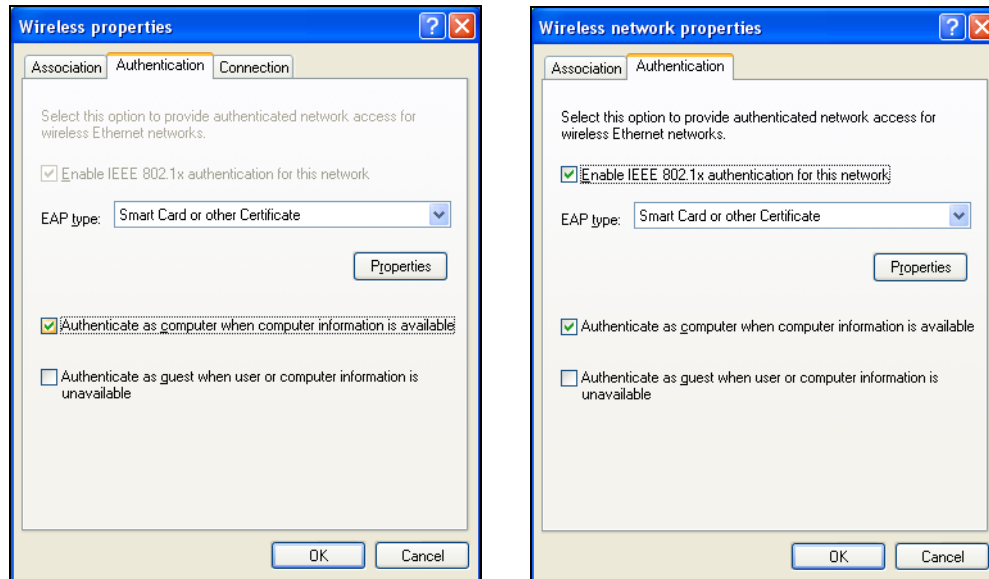
Table 28 Windows XP: Wireless (network) properties: Association

LABEL	DESCRIPTION
Network name (SSID)	This field displays the SSID (Service Set Identifier) of each wireless network.
Network Authentication	This field automatically shows the authentication method (Share , Open , WPA or WPA-PSK) used by the selected network.
Data Encryption	This field automatically shows the encryption type (TKIP , WEP or Disable) used by the selected network.
Network Key	Enter the pre-shared key or WEP key. The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN.
Confirm network key	Enter the key again for confirmation.
Key index (advanced)	Select a default WEP key to use for data encryption. This field is available only when the network use WEP encryption method and the The key is provided for me automatically check box is not selected.
The key is provided for me automatically	If this check box is selected, the wireless AP assigns the AG-225H v2 a key.
This is a computer-to-computer (ad hoc) network; wireless access points are not used	If this check box is selected, you are connecting to another computer directly.
OK	Click OK to save your changes.
Cancel	Click Cancel to leave this screen without saving any changes you may have made.

Authentication

Click the **Authentication** tab in the **Wireless (network) properties** screen to display the screen shown next. The fields on this screen are grayed out when the network is in Ad-Hoc mode or data encryption is disabled.

Figure 60 Windows XP: Wireless (network) properties: Authentication



The following table describes the labels in this screen.

Table 29 Windows XP: Wireless (network) properties: Authentication

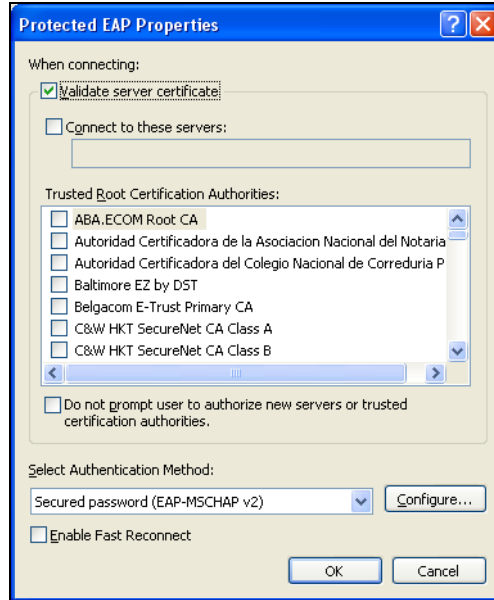
LABEL	DESCRIPTION
Enable IEEE 802.1x authentication for this network	This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to Open in the previous screen, you can choose to disable or enable this feature.
EAP Type	Select the type of EAP authentication. Options are Protected EAP (PEAP) and Smart Card or other Certificate .
Properties	Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the EAP type field.
Authenticate as computer when computer information is available	Select this check box to have the computer send its information to the network for authentication when a user is not logged on.
Authenticate as guest when user or computer information is unavailable	Select this check box to have the computer access to the network as a guest when a user is not logged on or computer information is not available.
OK	Click OK to save your changes.
Cancel	Click Cancel to leave this screen without saving any changes you may have made.

Authentication Properties

Select an EAP authentication type in the **Wireless (network) properties: Authentication** screen and click the **Properties** button to display the following screen.

Protected EAP Properties

Figure 61 Windows XP: Protected EAP Properties



The following table describes the labels in this screen.

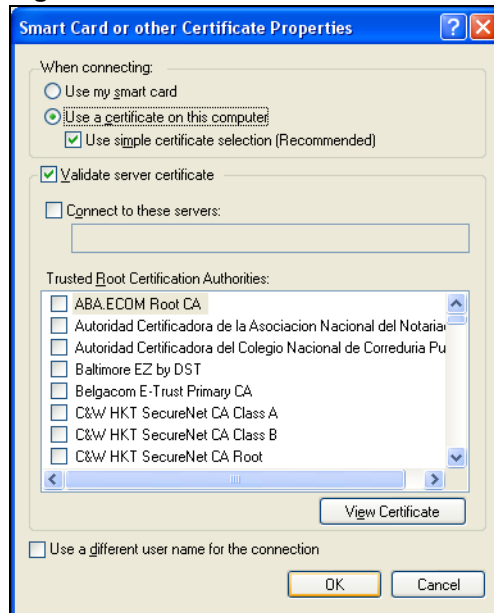
Table 30 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
Validate server certificate	Select the check box to verify the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Do not prompt user to authorize new server or trusted certification authorities.	Select this check box to verify a new authentication server or trusted CA without prompting. This field is available only if you installed the Windows XP server pack 2.
Select Authentication Method:	Select an authentication method from the drop-down list box and click Configure to do settings.

Table 30 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
Enable Fast Reconnect	Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down.
OK	Click OK to save your changes.
Cancel	Click Cancel to leave this screen without saving any changes you may have made.

Smart Card or other Certificate Properties

Figure 62 Windows XP: Smart Card or other Certificate Properties

The following table describes the labels in this screen.

Table 31 Windows XP: Smart Card or other Certificate Properties

LABEL	DESCRIPTION
Use my smart card	Select this check box to use the smart card for authentication.
Use a certificate on this computer	Select this check box to use a certificate on your computer for authentication.
Validate server certificate	Select the check box to check the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
View Certificate	Click this button if you want to verify the selected certificate.

Table 31 Windows XP: Smart Card or other Certificate Properties

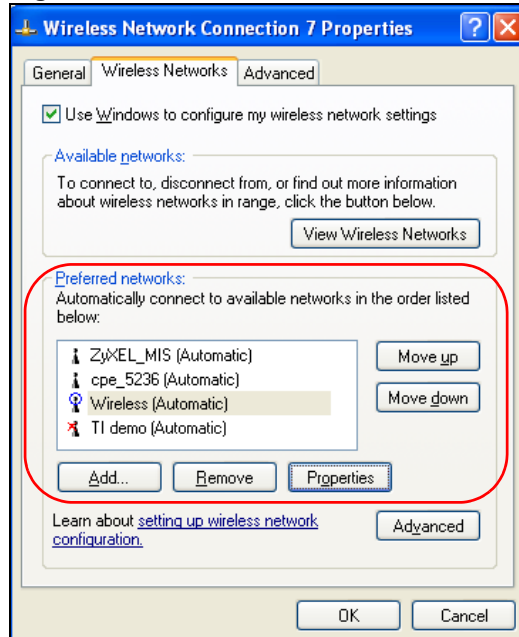
LABEL	DESCRIPTION
Use a different user name for the connection:	Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to.
OK	Click OK to save your changes.
Cancel	Click Cancel to leave this screen without saving any changes you may have made.

Ordering the Preferred Networks

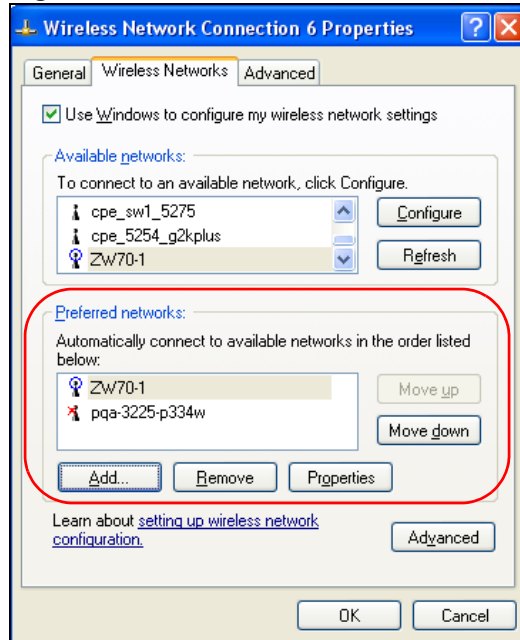
Follow the steps below to manage your preferred networks.

- 1 Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see [Figure 55 on page 77](#)). The screen displays as shown.

Figure 63 Windows XP SP2: Wireless Networks: Preferred Networks



Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the screen as shown.

Figure 64 Windows XP SP1: Wireless Networks: Preferred Networks

- 2 Whenever the AG-225H v2 tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or **Move down** to change its order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

APPENDIX D

Wireless Security

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 32 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

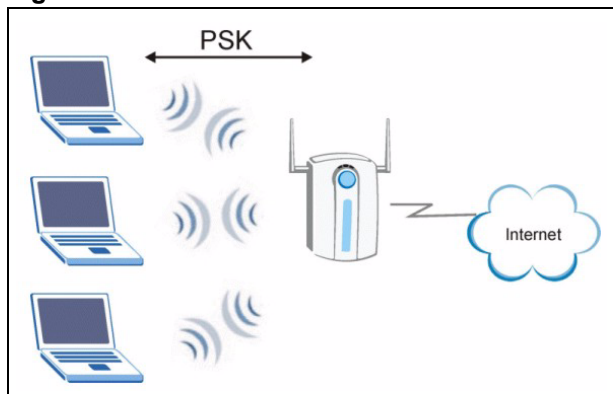
Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WPA(2)-PSK Application Example

A WPA(2)s-PSK application looks as follows.

- 1** First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2** The AP checks each client's password and (only) allows it to join the network if it matches its password.
- 3** The AP and wireless clients use the pre-shared key to generate a common PMK.
- 4** The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 65 WPA-PSK Authentication

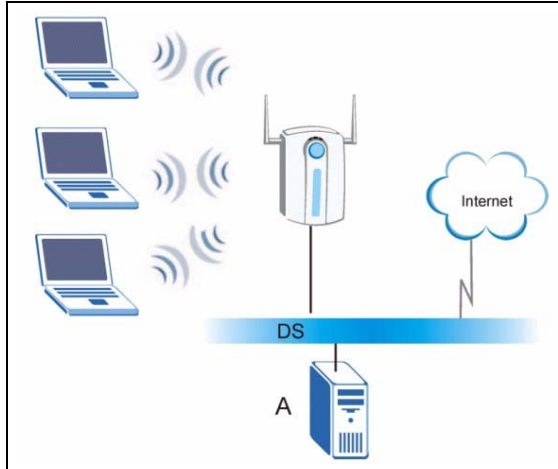


WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1** The AP passes the wireless client's authentication request to the RADIUS server.
- 2** The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3** The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 66 WPA(2) with RADIUS Application Example



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 33 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

APPENDIX E

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed. Windows 2000 and XP usually include TCP/IP.

Configure the TCP/IP settings in order to "communicate" with your network.

Windows 2000/XP

- 1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

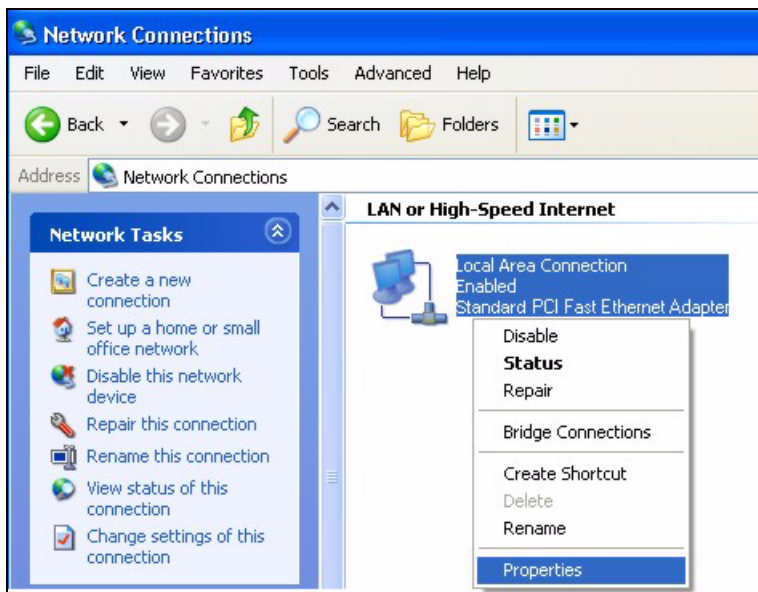
Figure 67 Windows XP: Start Menu



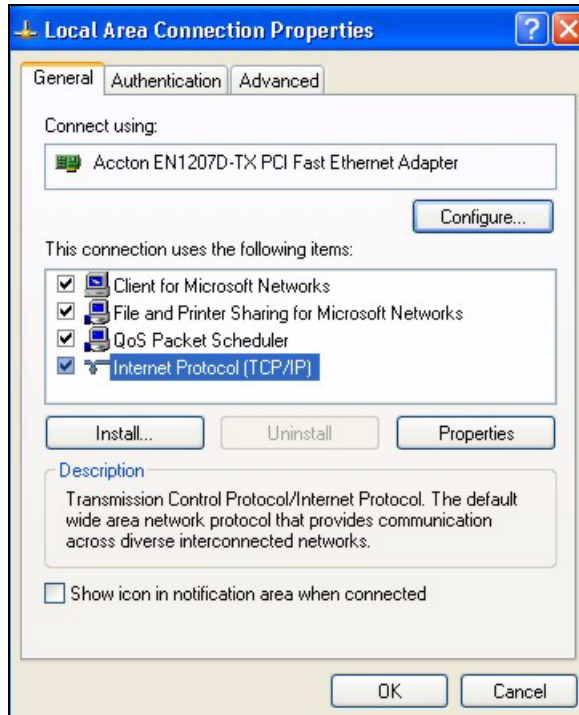
- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 68 Windows XP: Control Panel

3 Right-click **Local Area Connection** and then click **Properties**.

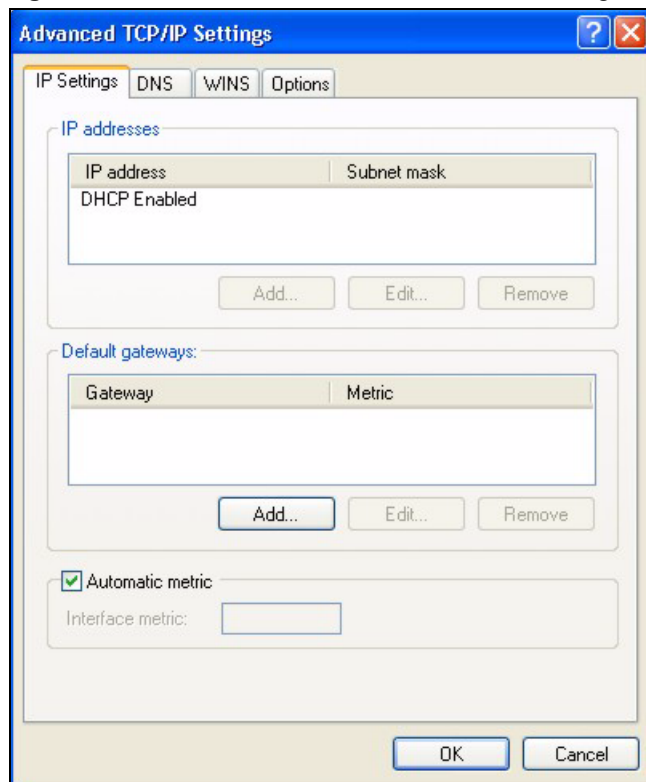
Figure 69 Windows XP: Control Panel: Network Connections: Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 70 Windows XP: Local Area Connection Properties

5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 71 Windows XP: Advanced TCP/IP Settings

- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

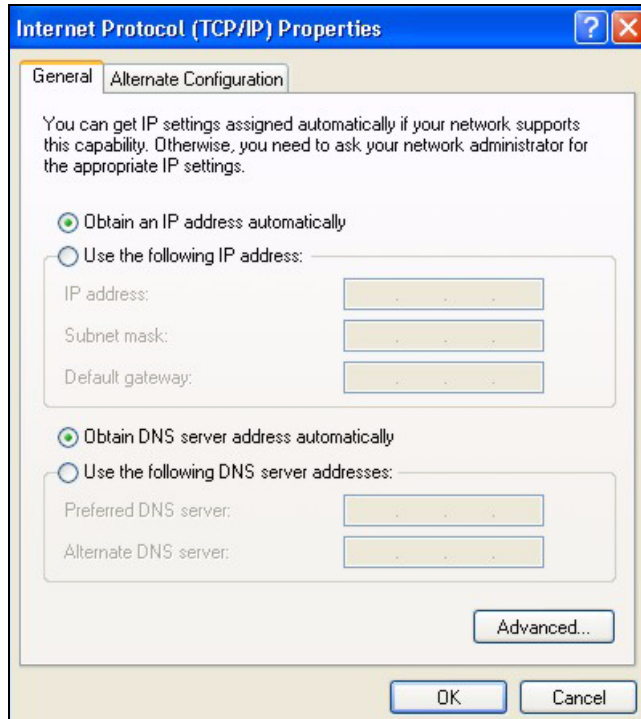
- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 72 Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.
- 10 Restart your computer (if prompted).

Verifying Settings

- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Index

A

About [63](#)
About your ZyXEL Device [19](#)
Access point (AP) [19](#), [25](#), [33](#)
Access point mode [21](#), [31](#), [40](#), [57](#)
 additional setup requirements [58](#)
Activating a profile [54](#)
Adapter [54](#)
Add new profile [50](#)
Ad-Hoc [20](#), [51](#), [53](#)
Advanced Encryption Standard (AES) [36](#), [89](#)
Advanced settings [54](#)
Antenna gain [60](#)
Antenna output power [59](#), [69](#)
AP. See also Access point.
Authentication method
 open system [35](#)
 shared key [36](#)
Authentication types [35](#)
Available network list [42](#)

C

CA (Certificate Authority) [46](#), [47](#), [88](#)
CCMP (Cipher block Chaining Message authentication code Protocol) [36](#)
Certificate Authority [88](#)
Certifications
 viewing [4](#)
Changing mode [21](#)
Channel [40](#), [42](#), [51](#), [70](#)
Configuration [59](#), [60](#)
 current [40](#)
Configuration method [22](#)
 Wireless Zero Configuration (WZC) [22](#)
configuration method
 Wireless Zero Configuration (WZC) [22](#)
Connection status [40](#)
Copyright [3](#)
Current status [58](#)
Customer Support [6](#)

D

Data encryption [43](#)
Data traffic statistics [41](#)
dBm [60](#)
Dimensions [69](#)
Disclaimer [3](#)
Driver version [63](#)
Dynamic WEP Key Exchange [88](#)

E

EAP Authentication [36](#)
Encryption [89](#)
Environmental specifications [69](#)

F

FCC [3](#)
Frequency [52](#)

G

Getting started [19](#)
Graphics icons key [18](#)

H

Hardware connections [22](#)
Hardware installation [22](#)
Humidity [69](#)

I

Icons [18](#)

IEEE 802.1x [36, 46](#)
Independent wireless workgroup [20](#)
Infrastructure [53](#)
Infrastructure mode [19](#)
Initialization vector (IV) [90](#)
Installation [22](#)
Interface [69](#)
Interference Statement [3](#)

K

Kbps (Kilobits per second) [41](#)
Kilobits per second (Kbps) [41](#)

L

LCD screen [19](#)
Link information [40, 58](#)
Link quality [41](#)
Login name [45](#)

M

MAC Filter [61](#)
MAC Filter action [62](#)
Message Integrity Check (MIC) [36, 89](#)
Mode
 current [21](#)

N

Network type [40](#)

O

Output power [59, 60, 70](#)

P

PA2-PSK [44](#)
Pairwise Master Key (PMK) [90](#)
Passphrase [35, 43](#)
Password phrase [35](#)
Physical specifications [69](#)
Power Saving Mode [55](#)
Preamble [55](#)
Product specifications [69](#)
Profile [40](#)
 activation [54](#)
 add new [49, 50](#)
 info [49](#)
 list [49](#)
 name [49](#)
profile
 delete [49](#)
 edit [49](#)
 information [49](#)

Q

Quick Start Guide [17, 22](#)

R

Radio frequency [53](#)
Radio interference [68](#)
Radio specifications [69](#)
RADIUS server [36](#)
Related Documentation [17](#)

S

Save power [55, 60](#)
Scan Info [51](#)
Security [59, 70](#)
 data encryption [35](#)
Security Parameters [92](#)
Security settings [60](#)
Sensitivity [70](#)
Signal strength [41, 42](#)
Site information [42](#)
Site survey [42](#)

- scan [42](#)
- security settings [43](#)
- Sleep mode [55](#)
- Soft AP [21](#)
- Software specifications [70](#)
- SSID [33](#), [40](#), [42](#), [58](#), [60](#)
 - hide [34](#), [60](#)
- Statistics [40](#)
- Support CD [17](#)
- Survey [42](#)
- Syntax conventions [17](#)
- System tray [22](#)

T

- Temperature [69](#)
- Temporal Key Integrity Protocol (TKIP) [36](#), [89](#)
- Trademarks [3](#)
- Traffic statistics [41](#)
- Transfer rate [55](#)
- Transmission rate [40](#), [50](#), [58](#), [70](#)
- Transmit key [43](#), [60](#)
- Trend Chart [41](#)
- Troubleshooting [67](#)
 - AP connection [67](#)
 - link status [68](#)
 - network communication [68](#)
 - starting ZyXEL Utility [67](#)

U

- Uninstalling ZyXEL Utility [63](#)
- Upgrading ZyXEL Utility [64](#)
 - important step [64](#)
- USB connection [19](#)
- User authentication [35](#), [90](#)

V

- Voltage [69](#)

W

- Web site [17](#)
- WEP [43](#), [60](#)
 - manual setup [44](#), [61](#)
 - passphrase [35](#), [43](#), [60](#)
 - security [35](#)
- WEP (Wired Equivalent Privacy) [35](#)
- WEP Encryption [43](#)
- WEP key [35](#)
 - automatic [35](#)
 - manual [35](#)
- Wi-Fi Finder [19](#)
- Wi-Fi Protected Access [36](#), [89](#)
- Windows XP [22](#)
- Wireless
 - independent workgroup [20](#)
- Wireless channel [33](#)
- Wireless client [25](#)
- wireless client [33](#)
- Wireless frequency [51](#)
- Wireless LAN
 - introduction [33](#)
 - overview [33](#)
 - security [34](#)
- Wireless LAN (WLAN) [33](#)
- Wireless mode [52](#)
- Wireless network [33](#)
 - location [19](#)
- Wireless standard [41](#), [69](#)
- Wireless station mode [40](#)
 - configuration [39](#)
- WLAN
 - Security parameters [92](#)
- WPA [36](#), [45](#), [89](#)
- WPA2 [36](#), [45](#), [89](#)
- WPA2-Pre-Shared Key [36](#), [89](#)
- WPA2-PSK [36](#), [89](#)
- WPA-PSK [36](#), [44](#), [89](#)
- WZC (Wireless Zero Configuration) [22](#)

Z

- ZyXEL Device Modes [21](#)
- ZyXEL Limited Warranty
 - Note [5](#)
- ZyXEL Utility [22](#)
 - accessing [23](#)
 - disable [22](#)
 - download [64](#)

help [23](#)
icon [22](#)
installation [22](#)
menu [39](#)
opening [23](#)
system tray icon [22](#)
upgrade [64](#)
version [63](#)